Security Lancaster | Lancaster University

# CYBER SECURITY CONTROLS EFFECTIVENESS

## A Qualitative Assessment of Cyber Essentials

*Security Lancaster — Lancaster University*

**Contributors:**
**Dr. Jose M. Such (Principal Investigator),**
**John Vidler,**
**Tim Seabrook,**
**Prof. Awais Rashid**
Security Lancaster
Infolab21 SCC
Lancaster University
Lancaster
LA1 4WA
United Kingdom

**Cite as:**
Such J.M., Vidler J., Seabrook T., Rashid A. Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials. Technical Report SCC-2015-02, Security Lancaster, Lancaster University, 2015.

**Acknowledgements:**
This Cyber Security research project was funded by the UK Government.

# Contents

# Executive Summary

## Findings

This report assesses the Cyber Essentials controls effectiveness in mitigating cyber-threats.

Two-hundred randomly selected internet-originating vulnerabilities are analysed for mitigation across four SME networks, with and without the Cyber Essentials controls in place. A network built from survey responses is used to assess the typicality of the SME networks, as well as to develop a broader understanding of typical SME network configurations and security-practice.

The aggregated results show that **without the Cyber Essentials controls none of the attacks assessed were mitigated on any network**. This, more than anything else should be understood by SMEs, taking no action to combat cyber threats simply isn't an option.

**With the CE tools, more than 99% of the vulnerabilities in SMEs interviewed were mitigated**, as shown in the figure below, which depicts the aggregated results across all cases studied. The approx. 1/3 of exploits only partially mitigated rely on hardware or software vendors to release patches succinctly and effectively to combat any vulnerabilities.

Once the vendor has released a security patch, the Patch Management component of Cyber Essentials ensures that the system returns to a secure state. However, up until a patch is released, there remains a vulnerability in the network. For this reason, it should be stressed for SMEs to frequently consider what services or software is installed, whether it is necessary, and whether a more secure alternative is available.

The few vulnerabilities not mitigated by Cyber Essentials, are as such because of fundamental hard-coded flaws in hardware or software that are unable to be updated or patched to a secure state.

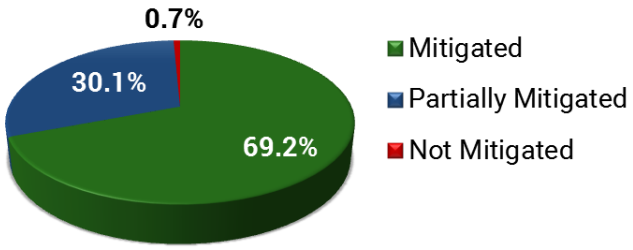



**Figure 1:** *Cyber Essentials Aggregated Vulnerability Mitigation Results*

## Recommendations

Although the Cyber Essentials tools have been shown to **successfully mitigate the vast majority of the attacks assessed**, it is important to note that only 'commodity-level' exploits (as defined by the Cyber Essentials Framework)[10] viable for a remote attack have been considered.

The scope of this report does not address vulnerability to insider threats, social engineering, physically proximate attackers or other targeted-attacks, it may be recommended that a follow-up study with a wider scope be carried out to investigate the risks from other forms of attack with the use of Cyber Essentials.

The '10 Steps to Cyber Security' report published by CESG[2] highlights that in order to maximise the security of a network, it is essential to not only consider the prevention of attacks with the use of tools, but to also **ensure that all employees are adequately educated in network security and treated with scrutiny**, through access logs and data-loss-prevention schemes, in order to achieve a secure business in the face of potential local and remote attacks. We would recommend that especially **for larger organisations** additional security measures such as these be put in place.

For hardware or software identified as inherently flawed, resulting in **unmitigatable** vulnerabilities, our recommendation is that these pieces of software or hardware be avoided at all costs when developing an SME network. In addition, a **global list of unsafe products** could be collectively developed and made publicly available. This relates to our last recommendation of integrating Cyber Essentials further with collective security approaches such as The Cyber-security Information Sharing Partnership (CiSP)[4]. These approaches keep SMEs with the latest information about vulnerabilities and other cyber-threat information.

# Introduction

Cyber Essentials was introduced as a government funded scheme, first published in April 2014 as an interest of national security to bolster UK security in cyberspace. The Cyber Essentials scheme was developed in collaboration with the Information Assurance for Small and Medium Enterprises (IASME) consortium, the Information Security Forum (ISF) and the British Standards Institution (BSI) as a set of basic technical security controls for organisations to utilize for the mitigation of the 'bottom 80%' of remote cyber-threats.[3]

The scheme, built to provide an implementable of the 10-steps to Cyber-Security[1], was released as part of the 2011 UK Cyber Security Strategy[16] and is being backed by the UK government as an organisational standard. Thus far it has been adopted by several large organisations including Vodafone, Hewlett-Packard (HP), BAE Systems, Virgin Media and Barclays[5].

The Cyber Essentials accreditation has been made mandatory, from October 1st 2014 for all suppliers of government contracts involving "the handling of sensitive and personal information and provision of certain technical products and services."[17]

The Cyber Essentials security controls are summarised as follows[7]:

**Firewalls and Gateways**
: These are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.

**Secure configuration**
: Ensuring that systems are configured in the most secure way for the needs of the organisation.

**Access control**
: Ensuring only those who should have access to systems to have access and at the appropriate level.

**Malware protection**
: Ensuring that virus and malware protection is installed and is it up to date.

**Patch management**
: Ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.

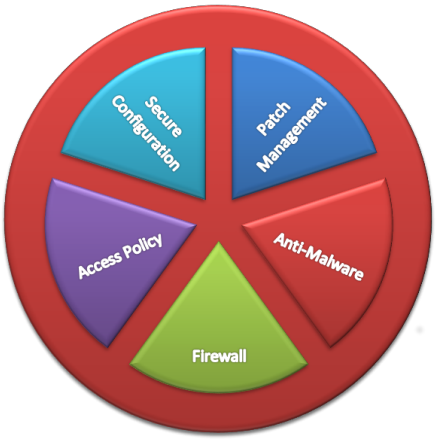



**Figure 2:** *Cyber Essentials Security Tools*

The intended scope of Cyber Essentials is outlined in the Cyber Essentials Scheme: Assurance Framework[10]. This states that the CE controls are considered as applicable to all sizes of Enterprise, as a base level of protection against cyber-attacks, upon which individual organisations may build on with further tools, network devices or protocols for the mitigation of targeted attacks. The CE Scheme is clear in its inclusion of 'Bring your own Device' network setups to scope, as well as Cloud-based services and off-the-shelf web applications. Bespoke IT systems such as in manufacturing and retail, are applicable to CE but hold additional vulnerabilities due to their nature that are not to be considered.

## Aims

The purpose of this report is to investigate the effectiveness of the Cyber Essentials controls in mitigating 'commodity-level' attacks attempting to exploit vulnerabilities in Small and Medium Enterprise (SME) networks.

A commodity-level attack has been defined by CESG[8] as:

> Any unauthenticated remote attack exploiting a known vulnerability with the use of tools and techniques openly available for download or purchase on the internet - and that do not require extensive specialist knowledge to conduct.[1]

To effectively assess Cyber Essentials it is firstly necessary to understand the typical network configurations of SMEs. Interviews with SMEs were carried out to build abstracted network models and a survey has been conducted to build a broader picture of SME network deployments. The survey results will help to develop our understanding of current security practice and cyber-awareness, as well as to build a general-case SME network with which to analyse the typicality of SMEs interviewed.

The networks modelled from collected data are to be considered with and without the use of the Cyber Essentials security controls, to comparatively establish the protection granted with the adoption of the CE scheme.

[1] This includes attacks utilising pen-testing software such as Metasploit, Kali and the Poison Ivy remote access tool, which are capable of scanning network nodes for publicly known vulnerabilities in the operating system, applications or services in use.

# Methodology

The scheme of work for this report has been split into the following sections:

- Collection of data through interviews and a survey regarding the implementation and deployment of networks in real-world SMEs, for use in designing paper-models to be analysed.
- Composition of a list of suitable vulnerabilities that contains applicable methods by which remote attackers can exploit commodity-level attacks.
- Assessment of vulnerability mitigation for SME networks with and without the use of the CE Tools.

## Data Collection

In order to analyse the effectiveness of the Cyber Essentials Security Tools four real-world SME networks have been modelled. Models have been composed using information gathered in interviews and abstracted to reduce redundant complexity and remove any linkage with the SME. In addition, a generalisable SME model was composed from Survey responses, to serve as a baseline network from which all SME networks may be adapted.

## Interviews

The interviews were composed with the goal of firstly understanding the layout or topology of the network deployed by an SME. To then build on the network configuration, it was important to understand how the network is used - where remote connections take place, how local services are utilised and how an attacker sees the network. Hardware vendors, operating systems and version numbers were considered to build a greater understanding of the network.

Additional questions were posed to examine the current state of security on the network, such as any security accreditations, previous breaches, and how often updates are rolled out.

## Survey

The Survey was constructed as a stripped-down questionnaire representing the essence of the questions posed in the Interviews. This included details of the number of workstations at the SME to gauge its size; the local and remote services available; the operating systems used on the service providers and workstations; the current security policies in place; and the respondents' awareness of the CE Scheme.

Two surveys were sent out, one to a secure list of SMEs in the NW Security Cluster[9], and another publicly to closed groups of security-interested SME representatives.

## Vulnerabilities

A total of 200 **random** vulnerabilities have been equally taken from two annual vulnerability lists of: CVE-2013 and CVE-2014 published by Mitre.[2] Any vulnerabilities found to be unsuitable for analysis have been replaced by a new candidate.

In this report, we use the Mitre organisation definition for a vulnerability, which they state as:

> *An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network. CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes entirely "open" security*

[2]CVE is sponsored by US-CERT in the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

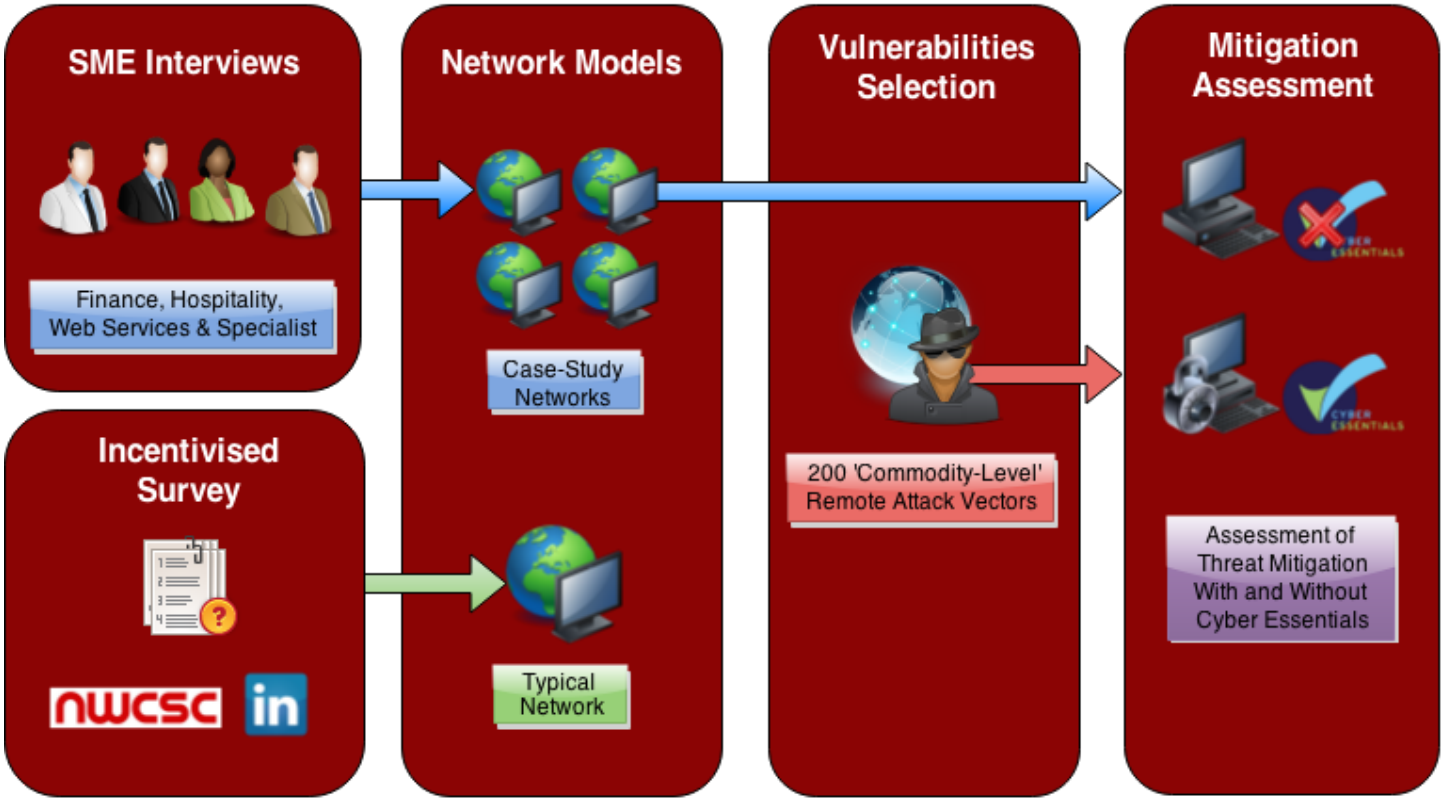



**Figure 3:** *Methodology for Assessing Cyber Essentials*

*policies in which all users are trusted, or where there is no consideration of risk to the system).*

(As shown on Mitre.org's Terminology page[6], in March '15)

To warrant a CVE entry into the Mitre list, individual vulnerabilities must place the affected system (or systems) in to a state which either:

- ... allows an attacker to execute commands as another user
- ... allows an attacker to access data that is contrary to the specified access restrictions for that data
- ... allows an attacker to pose as another entity
- ... allows an attacker to conduct a denial of service

## High-Profile Vulnerabilities

Three specific high-profile vulnerabilities were also taken in addition to the randomly chosen 200, and have been assessed to what extent the Cyber Essentials scheme would affect the vulnerability of SMEs in these situations.

Additionally, the applicability of these vulnerabilities to the SME networks we studied is included, along with the respective potential to harm operations.

## Mitigation Assessment

The Vulnerabilities chosen have been qualitatively assessed for mitigation with and without the use of the Cyber Essentials controls. The process considers each component of the controls in asserting whether each vulnerability would be mitigated, partially mitigated or not mitigated. The results are double-vetted to ensure correctness.

For each of the SMEs Interviewed, each of the vulnerabilities are assessed for applicability to that network configuration. In cases where the vulnerability is for a specific model of hardware, the network is deemed applicable if it uses a like-product from the same vendor. In cases where the vulnerability is in software, only those referencing software in-use or likely in-use (based on the SME's practice) are deemed applicable to the network.

# Analysis

The analysis of data collected has been split into sections, firstly each of the vulnerabilities have been assessed to ascertain their mitigation with and without the use of the Cyber Essentials controls, this supposes a case where any software or hardware source of a vulnerability is in use (i.e. a worst-case, fully inclusive assessment).

What follows is an analysis into the information gathered from interviews. Four SMEs from distinct industries are detailed in physical infrastructure and service usage, as well as current user access policies and existing security measures in place. A summary of the mitigation results in vulnerabilities in software and hardware used for each SME network configuration is included.

The full table for the applicability of all CVE vulnerabilities to each of the network structures can be found in the CVE Details section on page 19.

Finally, the data collected from the survey is analysed and used to develop a general-case network model, the SME networks are compared to this to better understand the nuances of each market sector, as well the overall typical configuration of SMEs.

## Full Vulnerabilities Assessment

Of the entire list of 200 vulnerabilities from 2013 and 2014, deemed as applicable to the study and chosen for analysis, 131 vulnerabilities were mitigated with the use of the Cyber Essentials Security Tools, 61 vulnerabilities were partially mitigated, and 8 were not mitigated.

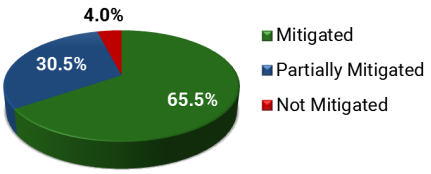



**Figure 4:** *Percentage of Full Vulnerabilities List Mitigated*

**Partially Mitigated** 59 of the 61 CVEs judged as partially mitigated are as such because they **rely of patches from third-party software or hardware vendors**, but that will be mitigated once a security fix has been released. Despite any level of security tools being deployed on a network, the security involved in using third party software unfortunately relies on the vendor's ability to identify potential areas of risk, as well as to quickly respond to security breaches as they become apparent with the release of patches. All software installed on an SME network should be periodically reviewed to decide whether it is necessary - or if there are more suitable and potentially more secure solutions available.

The other two partially mitigated vulnerabilities rely on website blacklisting, combined with avoiding vulnerable web browser software. A secure configuration without such a browser would mitigate this vulnerability, but as in the Web Development SME case study it may not always be possible to avoid the use of a specific software piece. In a case as this, website blacklisting is the only defence against the vulnerabilities.

**Not Mitigated - Secure Configuration** Some vulnerabilities have been found to be unmitigatable using the CE controls, in each of the found cases this is due to inherent flaws in a hardware device or software that can not be fixed by a security patch or firmware update.

For these devices that are fundamentally flawed from a cyber-security stand-point, it can be that no level of security tools on top of the network can aid in mitigation - rather the hardware should be replaced to ensure network security. It may be possible for a public list of all such devices to be developed as part of the government cyber-security scheme - to serve as a device-blacklist for SMEs.

## Case Studies

Four SMEs were interviewed to build paper-models upon which the Cyber Essentials controls may be assessed. Some detail on the physical structure, usage and existing security of each network is provided.

- SME Network One represents a finance specialist SME using a combination of externally managed services for banking in addition to internal, remotely accessible internal services for employees.
- SME Network Two represents a specialist SME utilizing an off-site remotely managed server for administrator services, and cloud-based services for employees.
- SME Network Three represents a web services SME that accesses client servers frequently, and utilises cloud-based services daily.
- SME Network Four represents a hospitality services provider with a very small company network co-located with a very large guest network component, where all of the services are remotely managed and located.

### SME Network One - Finance Sector

**Physical Infrastructure** The company interviewed comprised around 20 employees, located at 3 sites nationally.

Remote workers connect over normal internet connections, both residential and commercial, and use both VPN and non-VPN traffic (specifically web traffic on port 80) to access services supplied by the company.

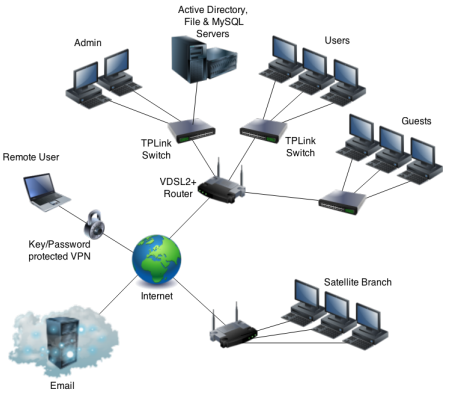



**Figure 5:** *SME-1 Network*

The hardware at the head office (where the interview was carried out) consists of equipment by 3Com, Draytek, BT and Heuwai for infrastructure components. Employees use a range of machines bought between 2011 and 2014 comprising a mix of Dell and Lenovo PCs.

As most of the infrastructure is passive (most of the traffic is handled by a single 3Com BaseT-1000 switch) the firmware on the equipment is unchanged from purchase, if any firmware is present at all.

**Services** At the head office site, a Windows File Server (SAMBA) server provides local file sharing, and allows remote users to access the same files via VPN. The mail server, a Microsoft Exchange Server is an off-site, deployment, managed by an external company, but is a dedicated server for only this company.

Additionally, a web service and database server is run from a server at the site. This provides both local HTTP access to the database it runs, as well as having firewall rules put in place to allow external access to the same system for off-site employees.

Numerous other pieces of banking software are run on bank-owned, remote servers, and are accessed and secured via combinations of smart cards and PIN entry devices, also supplied by the banks.

**User Access** Employees are permitted to access the internet from both their individual workstations, and additional devices, such as smart phones (although technically this is not permitted by policy, but this policy is not strictly enforced). Internet access is, however, slightly filtered, with access to Facebook being blocked by the router.

Access logs for any network operations are not created, and any machine in the office can access the network, with no isolated islands.

User accounts can be migrated between machines, via a Domain Controller, but in practice this is unlikely to actually happen, with users generally using their own machines.

**Operating systems** Locally, everything is Windows 7, the remote site uses Windows 7. 2 remote machines are Windows 8.1.

**Mitigation of applicable vulnerabilities** Of the 200 listed vulnerabilities, 119 were applicable to the first SME network.

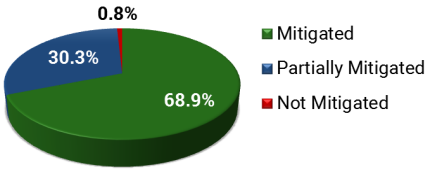



**Figure 6:** *SME-1 Vulnerability Mitigation*

Because much of this SMEs operations are done via browser-based interfaces to other financial companies (such as banks), it places them in the firing line for a large number of the browser based attacks. Furthermore, as some banks require specific browser versions for their interfaces to work, they end up with several different browsers, with several versions of each to cover all their requirements, opening them up multiple times to browser-based vectors.

Additionally, the heavy use of SSL-based communication places them in a position where any SSL vulnerabilities affect them too.

## SME Network Two - Specialist Group

**Physical Infrastructure** The second SME participant employs 20-25 based across multiple offices in one building.

Employees may bring their own devices, or use a workstation provided. Workstations are connected to one of four switches via Ethernet, and share a virtual LAN with other employee devices. An off-site server containing sensitive data is accessible only to administrators via SSH.

Network Equipment includes an external Dell PowerEdge Server, four TPLink Switch Access Points, and a TPLink DHCP Router.

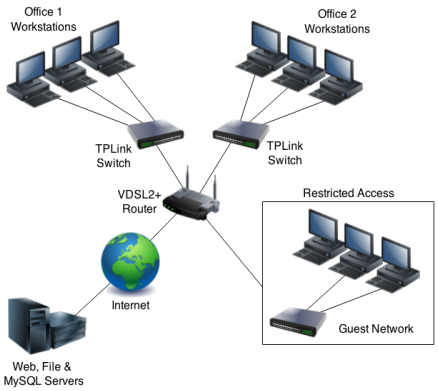



**Figure 7:** *SME-2 Network*

**Services** Employee devices sharing the network can use Windows Folder Sharing. Employee devices include OSs: OS X, Windows XP, Windows 7 & Windows 8 with auto-updates enabled.

Some Employee use of VPN to connect to another network for a data service. All other services are provided by cloud servers via HTTPS: Email, Files & Database as well as management tools, these are used daily.

**User Access** Employees have no restriction on their internet access, and may use their own equipment. Administrators often access a remote server database and file store, acting as a web server. Guests may access a separate Wi-Fi network through the same access points as other office workers, but do not share the same virtual LAN as employees. Wi-Fi access logs are gathered, but no other user activity. Employees can access the network from any machine, but the SME's policy is that all machines should have anti-malware and strong passwords which are recommended to be changed periodically, with the employee machines configured to automatically lock after a period of inactivity.

**Mitigation of applicable vulnerabilities** Of the 200 listed vulnerabilities, 79 were applicable to the second SME network.

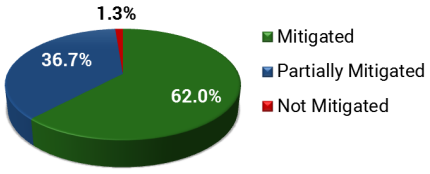



**Figure 8:** *SME-2 Vulnerability Mitigation*

The specialist SME had the fewest overall potential vulnerabilities, largely owed to a higher reliance on cloud-based services. Although this reduces the risk from inherent vulnerability in a network, responsibility is handed onto the service provider chosen. A certified and reputable cloud services provider should thus be sought to ensure protection through the entire chain.

## SME Network Three - Web Development

**Physical Infrastructure** SME-3 employs 10 workers based in one building.

Employees are restricted from using their own devices, unless it is validated by the company head - in which case no others may share that device. Workstations are connected to one switch via Ethernet, and share a virtual LAN with other employee devices.

Network Equipment includes an external Dell PowerEdge Server, one TPLink Switch Access Point, and a TPLink DHCP Router.

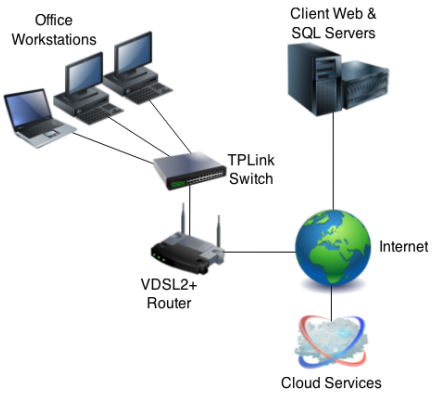



**Figure 9:** *SME-3 Network*

**Services** Employee devices sharing the network can use Windows Folder Sharing. Employee devices include OSs: OS X, Windows 7 & Windows 8 with auto-updates enabled.

All services are provided by cloud servers via HTTPS: Email, Files & Database as well as management tools, these are used daily.

**User Access** Employees have no restriction on their internet access, and commonly use all major browsers for compatibility testing.

Guests are not permitted on the network, but may join a 'guest' network through the same access points with a mobile device. Wi-Fi logs and Cloud Service Access logs are gathered, and actively monitored. Employees can access the network from a validated machine, but the SME's policy is that all machines should have anti-malware and

strong passwords which are recommended to be changed periodically, with the employee machines configured to automatically lock after a period of inactivity.

**Mitigation of applicable vulnerabilities** Of the 200 listed vulnerabilities, 116 were applicable to the second SME network.

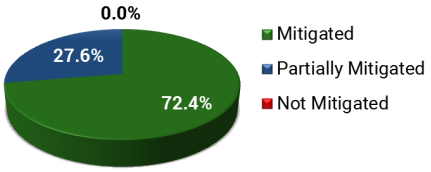



**Figure 10:** *SME-3 Vulnerability Mitigation*

The requirement for web development SMEs to operate across multiple web browsers on various versions to test and build a customer's website means that the network accumulates all vulnerabilities in web browsers. As this is a specialist case, a recommendation for web development organisations could be to use one up-to-date browser for general use. A bespoke policy may then be put in place:

*When working on alternative browsers, employees should only access client pages, where the developer has control of the web-content.*

## SME Network Four - Hotel Services

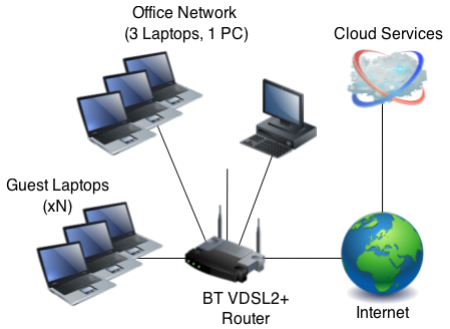



**Figure 11:** *SME-4 Network*

**Physical Infrastructure** This company is located at a single site, and has equipment composed of a single desktop PC, and 2 company laptops running on a ADSL router - this same router also provides the internet connection for the guests. An alternative router is available as a manual fall-back connection to the internet, but is available only to company equipment.

The guest network is split from the office network through secondary access point names filtering traffic in to a separate VLAN internal to the router.

**Services** No local servers are present to provide any service to employees or guests on the network.

File storage is provided through on-line services including Dropbox and Skydrive. A standalone web-server owned and managed externally runs the company website, and bookings are managed via a globally accessible website.

All the services are accessed with SSL secured connections (HTTPS, mainly).

**User Access** User access is not mediated in any way, and any site can be accessed from any computer. Guests have no restrictions placed on their network usage either.

**Operating systems** The company uses iOS for their mobile devices, and Windows 8.1 for the office desktop and laptop PCs. Guests can bring their own equipment, so will be a mix of all operating systems currently available, including Windows, Linux, Mac and others.

**Existing Security Measures** Beyond the router's separation between the guest and office networks no other network security measures are in place. The office PCs do have automatic patch installation configured, however, and have the Kaspersky antivirus suite installed.

**Mitigation of applicable vulnerabilities** Of the 200 listed vulnerabilities, 103 were applicable to the second SME network.

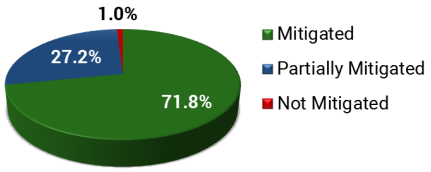



**Figure 12:** *SME-4 Vulnerability Mitigation*

Similarly to SME 1, SME 4 requires the use of web browsers for bookings and reception of guests, so enables a wide variety of attack vectors through the web.

Thankfully, the services and servers they connect to are run by larger corporations, which will hopefully have implemented at least Cyber Essentials-grade security and protection, so the actual risks should be minimal.

For the purposes of this report, however, we assume that if this company has not implemented Cyber Essentials, then the services they use must also not have, leaving them open to attack.

## Survey Responses

Data gathered from survey responses affords a much broader look at the typical network deployments and practice in SMEs. The full results from 17 participants may be found in the Survey Responses section on page 27.

**Physical Infrastructure** The majority of respondents belong to SMEs with 0-9 workstations on site, this is related to the size of an organisation - and could be considered representative of businesses across the UK.

**Services** Local - File, Email, Database and Domain Servers are the most common local service providers all present in more than 1/3rd of SMEs. Remote - Email, web hosting and file-sharing are the most common services provided remotely.

**User Access** More than half of SMEs permit employee's own devices to be used in the workplace, for organisations such as these it is important to ensure that employee machines receive the same level of protection as the rest of the work network - as one vulnerable machine allows vulnerability into the whole company.

**Existing Security Measures** Of the survey respondents, most SMEs have a firewall, password policy and data-loss prevention scheme in place. These are the most common security measures in place for the SMEs contacted, below this is access control, malware protection and finally patch management which is present in a little over half of organisations.

Almost two-thirds of survey participants were previously aware of Cyber Essentials.

## Survey Respondents Network

The network built from Survey Respondents data considers the overall response, in order to build a network easily adaptable to match that of the majority of SME network configurations.

Locally, Email and File servers have been represented, with domain controller capabilities represented in a network ADSL Router. Remotely, a web server is depicted, but remote services may also include database usage, email and other web services.

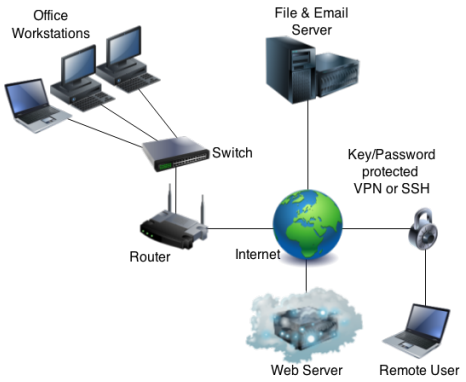



**Figure 13:** *Adaptable Survey-Response Network*

## Typicality of Case-Study SMEs

Within the Survey Respondents network, aspects of each of the interviewed SME networks is apparent.

The **Finance** SME network shares a local file server, as sensitive information needs to be kept and processed by the organisation. Any SME handling sensitive information will be likely to strongly consider using local file servers.

The **Specialist** SME shares with the survey respondents data it's use of SSH to connect remotely to services, SSH is an important tool for accessing sensitive date while at home, or data that is stored remotely the workplace.

The **Web Development** SME requires employees to connect to many web servers remotely, the survey respondents match this case with the use of external web-hosting services. That being said, in the general-case this server is more likely to be the SME's own web-hosting solution, rather than a clients.

The **Hotel Services** SME represents a very basic local network using only cloud-based services remotely. This is becoming an increasingly popular trend for SMEs, as cloud-services are often easier to set up and cheaper to maintain. This is also representative of many SMEs with little-to-no online presence.

# Analysis of Cyber Essentials on High Profile Vulnerabilities

The following sections detail three of the high-profile vulnerabilities to hit the popular media in late 2014 to early 2015. These are of particular note, as while they may not be the most damaging of attack vectors (although some are very serious) they have caught the attention of the public, and SMEs would be under pressure to ensure that they were protected.

With this in mind, we analyse how effective the Cyber Essentials security controls are at tackling these high-profile vulnerabilities.

## "ShellShock"

Also known by the name "BashDoor", Shellshock hit the news as it attacked the Linux server environment, and did so in a particularly effective manner.

> *GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.*
>
> CVE-2014-6271[13]

The exploit allowed attackers to directly execute arbitrary shell commands on a compromised system by altering environment variables. However, the bug was not enough by itself to actually enable attackers to compromise a system, but allowed access via other services. While the exploit is only effective if the bash environment can be altered, the results can be devastating, as it lays bare the entire system to many other forms of attack.

The threat was particularly insidious for SMEs who used Linux/Unix based servers for services, mail servers as an example, as they would potentially have no idea that they had been compromised.

## "Heartbleed"

Appearing in April, 2014; the CVE-2014-6271 (aka. "Heartbleed") bug allowed attackers to directly read the active memory of a target machine through buffer over-read. This then allowed attackers to access private credentials (or indeed, anything else) in the RAM of the target.

As described in the original CVE report:

> *The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.*
>
> CVE-2014-6271[12]

As OpenSSL is a core part of many applications and services, both in the open and closed source world, this vulnerability had the potential to damage a huge number of systems. At the time of release, various sources (including, for example Netcraft[15]) that up to 17% of trusted SSL-certified servers were vulnerable to the attack.

Depending on how the SME in question operates, the threat this particular CVE posed (and indeed, still poses with still as yet to be updated servers still online with the vulnerability) is difficult to discern. Obviously, the vulnerability is serious, but the ability of individual SMEs to detect and correct this flaw will vary greatly depending on the individual deployments.

Larger companies with their own Linux/Unix servers may have be able to deploy the patched OpenSSL version as soon as the patch was available, but smaller businesses, or those with more cloud-based services, may not have access to the software running on the servers they use, and may be at the mercy of the respective operators to implement the fix. Because of this, patch management only partially remedies this vulnerability, and other protection methods from the Cyber Essentials guidelines, such as securing configurations or controlling access will have unknown effects.

It is vulnerabilities such as this that pose the greatest threat to SME networks, as the methods to fix the issue are often outside the control of the company, potentially leaving them vulnerable far longer than one would expect.

## "Superfish"

> *The SDK for Komodia Redirector with SSL Digestor, as used in Lavasoft Ad-Aware Web Companion 1.1.885.1766 and Ad-Aware AdBlocker (alpha) 1.3.69.1, Qustodio for Windows, Atom Security, Inc. StaffCop 5.8, and other products, uses the same X.509 certificate private key for a root CA certificate across different customers' installations, which makes it easier for man-in-the-middle attackers to spoof SSL servers by leveraging knowledge of this key, as originally reported for Superfish VisualDiscovery on certain Lenovo Notebook laptop products.*
>
> CVE-2014-6271[14]

This vulnerability is particularly interesting, as the software causing the issue was effectively brokered by a trusted hardware vendor, namely; Lenovo. Because the issue was part of the 'normal configuration' for the equipment, it remained undetected for a long time, and hints that there may be further breaches in security as yet undiscovered in both Lenovo, and other manufacturer's equipment.

The vector is through the SuperFish software essentially breaking the chain of trust for SSL certificates by installing a self-signing certificate in to the list of trusted certificates on the host machine. This allows an attacker to simply sign their own code via the same

certificate, which itself can be easily gathered from any other machine running SuperFish, and they have full access to any SSL-secured connection from the target machine.

Thankfully, while the risks to users and SMEs was high, the fix is a simple, one-time run of a removal tool provided by Lenovo themselves[11], and is mitigated fully through the Cyber Essentials patch management advice.

## Threat Analysis

**ShellShock** Without Cyber Essentials in place, SME 1 and 2 would be at risk from 'Shellshock, as they both operate Unix/Linux based systems that would require patching to plug the security issue. The extent at which SMEs 3 and 4 are vulnerable to this issue is unclear, as their large dependency on outside service providers leaves them in a position where they are both unable to determine their vulnerability and additionally unable to remedy it.

With Cyber essentials, SME 1 and 2 would be fully protected, and it is likely that SME 3 and 4 are also protected if the external providers also use a Cyber Essentials or other security and patching schemes.

**Heartbleed** The 'Heartbleed' bug is another vulnerability that without Cyber Essentials guidelines being followed, would have laid companies external-facing services open to malicious attackers.

In all cases, however, each SME can be fully protected with a combination of patch management, firewalling and application of access controls from the Cyber Essentials guidelines.

**SuperFish** All of the SMEs we interviewed could be exceedingly vulnerable to the 'Superfish' issue without Cyber Essentials, as much of their operations revolve around SSL encrypted communications. A break in the chain-of-trust for their certificates would allow an attacker to man-in-the-middle their communications.

Normal system updates would have failed to remedy the situation, as the fix provided by Lenovo consisted of a tool to be run in addition to the normal operating system patches. It is further debatable how effective Cyber Essentials patch management would have been in plugging this vulnerability, as it would require that the administrators be aware of the issue and know of the patch, rather than simply following 'normal' patching guidelines. Assuming that the persons responsible for the equipment are aware of the issue, however, then Cyber Essentials patch management fully mitigates this issue.

# Conclusions

The Cyber Essentials Security Tools have been shown to mitigate, or to mitigate as soon as a patch is released, all vulnerabilities from remote attackers that do not exploit fundamentally insecure software or hardware. Of the two-hundred vulnerabilities collected, eight exploits were not able to be resolved with the deployment of security patches, for vulnerabilities such as these the only mitigation available is simply not to install the compromised systems. To help prevent deployments being susceptible to attacks on faulty systems, it may be recommended that a blacklist of such items is composed for public reference.

**Scope** It is important to consider that the scope of this study covers only internet-based commodity-level attacks, and although the Cyber Essentials tools performs very well in mitigating this, it does not represent full security. There is an increasingly identified **risk from insiders** that also requires attention, not least malicious acts, but also from users unknowingly compromising security.

The SMEs interviewed represent organisations from a range of market sectors, in web development and online presence, specialist scientific services, the hospitality industry and finance.

## Additional Tools

The 10 Steps to Cyber Security[2] identifies additional security measures that support the Cyber Essentials Scheme well, to deliver additional security through indirect measures such as User Education, Awareness, along with Network and Systems Monitoring. These additional measures would serve to bolster cyber security through fortifying each employee of the SME with necessary knowledge on safe practice, it's importance, and some technical basic understanding - just as they may be versed in environmental awareness. Network and Systems Monitoring allows for remote user logins, as well as file access and activity to be logged. For very small networks this may be currently infeasible, as the extra manpower or finances required for such a system are costly. However, for large organisations additional monitoring capability should be explored as a future extension to the Cyber Essentials, not just to identify and mitigate malicious action, for more bespoke and sophisticated attacks than those reported on, but to also aid in providing evidence for any potential cyber-crime investigations.

There exist some collective approaches to improving cyber-security, a notable example of this is The Cyber-security Information Sharing Partnership (CiSP)[4]. The partnership aims to benefit all members by providing real-time updates on issues of cyber-security and discovered vulnerabilities, as well as best-practice guides and other cyber-threat information. It would be beneficial for more organisations to belong to cyber-security collectives like this, creating networks of informed individuals working together to tackle cyber-crime. This would be particularly useful to quickly identify potential vulnerabilities and possible patches, which, as shown in this report, is critical for the CE patch management security control to fully mitigate related vulnerabilities.

An important note to be made is toward the security of business affiliates and service providers. Even if an SME has Cyber Essentials in place, any use of cloud-services relies on the vendor's security controls for threat mitigation. In other words, cloud-email, accounting and any other cloud-based or remote services are only as secure as the service provider makes it. In general, cloud-providers should be holding a high level of scrutiny to their security practice, and should be encouraged to certify their protection. Hewlett-Packard(HP) has taken this further, and has begun to strengthen it's entire supply-chain ( 600 SMEs) with the Cyber Essentials accreditation. This provides protection across the entirety of Hewlett Packard's operations, as well as it's affiliates. This should be a goal for organisations of all sizes, minimising the risk from cyber-threats by ensuring all trading partners uphold the same high levels of security.

## Cyber Essentials Controls

Of the five current Cyber Essentials Controls, Patch Management was considered to aid in the mitigation of the highest proportion of remote attacks (87.5 %), counter-intuitively the Survey responses had patch management ranked last in use for SMEs. The highest currently used controls could be seen as those providing the most intuitive or easily understood protection: Data loss prevention, strong passwords and firewall. While patch management isn't necessarily understood by individuals as a tool to greatly improve cyber-security.

Anti-Malware was useful in mitigating the least (10 %) vulnerabilities. It is however important to note that Anti-Malware is largely the only security tool that may routinely scan the network hardware and software, as well as any items downloaded from the internet or as email attachments. This serves as a last line of defence, and as such is vital to an organisation's cyber-safety.

## Recommendations

To further improve cyber-security across the UK, we recommend that:

1. Collective approaches to cyber security should be further encouraged. In particular, a governmental/collective approach to identifying inherently flawed products should be developed. This could be in addition to or as an extension to current initiatives like CiSP, which can make a difference in detecting and reacting on potential vulnerabilities in a timely manner.

2. Further research into the mitigation of other cyber-threats is carried out to explore the risk from insider-threats and targeted attacks.

3. Further employee education is strongly encouraged, specially, to be able to tackle these other types of attacks mentioned above, which were not under the scope of this report.

# References


[1] Centre for the Protection of National Infrastructure CESG, Cabinet Office, Innovation Department for Business, and Skills. Cyber security guidance for business. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility, September 2012.

[2] Centre for the Protection of National Infrastructure CESG, Cabinet Office and Innovation & Skills Department for Business. 10 steps to cyber security. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility, September 2012.

[3] Innovation CESG; UK Trade & Investment; Prime Minister's Office, 10 Downing Street; Centre for the Protection of National Infrastructure; Government Communications Headquaters; UK Trade & Department for Business and Skills. Cyber security boost for uk firms. https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms, January 2015.

[4] Centre for the Protection of National Infrastructure CiSP, CERT-UK and Innovation & Skills Department for Business. Cyber-security information sharing partnership (cisp). https://www.cert.gov.uk/cisp/, March 2013.

[5] CREST. Cyber essentials certified companies. http://www.cyberessentials.org/list/, March 2015.

[6] CVE.Mitre.org. Terminology - mitre.org. http://cve.mitre.org/about/terminology.html.

[7] Cyber Essentials. Cyber essentials scheme - overview. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[8] CESG; Cabinet Office; Centre for the Protection of National Infrastructure; Department for Business Innovation & Skills. Common cyber attacks: Reducing the impact. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf, January 2015.

[9] UK Cyber Security Forum. North west cyber security cluster. http://www.ukcybersecurityforum.com/index.php/cyber-security-clusters/north-west-‘-cluster, 2015.

[10] HM Government. Cyber essentials certified companies. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400914/bis-15-72-cyber-essentials-scheme-assurance-framework.pdf, January 2015.

[11] Lenovo. Superfish uninstall instructions. http://support.lenovo.com/us/en/product_security/superfish_uninstall.

[12] Mitre.org. Cve-2014-0160 aka. heartbleed. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160, 2014.

[13] Mitre.org. Cve-2014-6271 aka. shellshock. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271, 2014.

[14] Mitre.org. Cve-2015-2077 aka. superfish. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2077, 2015.

[15] Netcraft. Half a million widely trusted websites vulnerable to heartbleed bug. http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html, April 2014.

[16] Cabinet Office. The uk cyber security strategy - protecting and promoting the uk in a digital world. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, November 2011.

[17] Cabinet Office and The Rt Hon Francis Maude MP. Government mandates new cyber security standard for suppliers. https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers, September 2014.

# Cyber Controls Applicability

| CVE | SME1 | SME2 | SME3 | SME4 | Idealised | No CE | With CE |
|---|---|---|---|---|---|---|---|
| CVE-2013-0008 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration (User Policy), Anti-Malware |
| CVE-2013-0022 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-0084 | y | y | y | n | y | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-0140 | y | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0149 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-0172 | y | n | n | n | n | Not Mitigated | Mitigated - User Access (Strong Password), Patch Management |
| CVE-2013-0174 | n | n | n | n | n | Not Mitigated | Mitigated - Access Policy (Strong Password), Firewall, Patch Management |
| CVE-2013-0199 | y | n | n | n | n | Not Mitigated | Mitigated - Patch Management & Secure Configuration |
| CVE-2013-0253 | n | n | y | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Server) |
| CVE-2013-0270 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0481 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0598 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0619 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0633 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration (Secure Browsing), Firmware Management |
| CVE-2013-0649 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration (Secure Browsing), Patch Management |
| CVE-2013-0746 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-0753 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-0787 | y | y | y | y | n | Not Mitigated | Mitigated - Patch Management |
| CVE-2013-0909 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1035 | y | y | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-1102 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-1140 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |
| CVE-2013-1144 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management & Firewall |
| CVE-2013-1153 | y | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration |
| CVE-2013-1181 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-1303 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-1384 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration (Secure Browser) |
| CVE-2013-1388 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration |
| CVE-2013-1450 | y | n | y | y | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2013-1472 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration (Access Policy) |
| CVE-2013-1553 | y | n | y | y | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1620 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Patch Management & Firewall |
| CVE-2013-1627 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1638 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1669 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1676 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1700 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management, Anti-Malware |
| CVE-2013-1734 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-1777 | n | n | y | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2013-2319 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Firewall, Secure Configuration (Secure Browser), |
| CVE-2013-2340 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |

| CVE | SME1 | SME2 | SME3 | SME4 | Idealised | No CE | With CE |
|---|---|---|---|---|---|---|---|
| CVE-2013-2350 | n | y | n | n | y | Not Mitigated | Partially Mitigated - Patch Management & Firewall |
| CVE-2013-2492 | y | n | y | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-2507 | y | n | n | n | n | Not Mitigated | Partially Mitigated - Firmware Management, Anti-Malware |
| CVE-2013-2736 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-2780 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-2803 | n | n | n | n | n | Not Mitigated | Mitigated - Strong Passwords, Patch Managements |
| CVE-2013-2824 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-2826 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-2920 | n | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-3064 | y | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3116 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3137 | y | y | y | y | n | Not Mitigated | Mitigated - Anti-Malware, Secure Configuration (Don't Install) |
| CVE-2013-3194 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3199 | y | n | y | y | y | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3201 | y | n | y | y | y | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3206 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3280 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management & Secure Configuration |
| CVE-2013-3387 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-3417 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3632 | y | y | y | n | n | Not Mitigated | Mitigated - Access Policy (Strong Password), Firewall |
| CVE-2013-3656 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-3856 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Firewall, Anti-Malware |
| CVE-2013-3860 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-3893 | y | n | y | y | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration - no JS. |
| CVE-2013-3897 | y | n | y | y | n | Not Mitigated | Mitigated - Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-3900 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-3905 | y | y | n | y | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |
| CVE-2013-4223 | y | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |
| CVE-2013-4436 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2013-4478 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration |
| CVE-2013-4529 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-4555 | y | n | y | y | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-4776 | y | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Patch Management |
| CVE-2013-4782 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |
| CVE-2013-5057 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-5369 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management & Secure Configuration |
| CVE-2013-5428 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-5431 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-5494 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration |
| CVE-2013-5507 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2013-5536 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2013-5559 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-5561 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration |
| CVE-2013-5751 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management & Secure Configuration |
| CVE-2013-5757 | n | n | n | n | m | Not Mitigated | Mitigated - Firewall |
| CVE-2013-5828 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |

| CVE | SME1 | SME2 | SME3 | SME4 | Idealised | No CE | With CE |
|---|---|---|---|---|---|---|---|
| CVE-2013-6167 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Access Control, Secure Configuration (Cookie-deletion) |
| CVE-2013-6188 | y | y | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-6284 | n | n | n | n | n | Not Mitigated | Not Mitigated - Secure Configuration (Don't install) |
| CVE-2013-6396 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Server) |
| CVE-2013-6475 | n | y | y | n | n | Not Mitigated | Mitigated - Anti-Malware, Firewall, Patch Management |
| CVE-2013-6660 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2013-6699 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Secure Configuration |
| CVE-2013-6702 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2013-6979 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2013-6994 | n | n | y | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2013-7004 | y | n | n | y | n | Not Mitigated | Mitigated - Firewall, Secure Configuration, Firmware Management |
| CVE-2013-7043 | n | n | n | y | n | Not Mitigated | Partially Mitigated - Firmware Management |
| CVE-2013-7389 | y | n | n | y | y | Not Mitigated | Mitigated - Firewall, Secure Configuration, Firmware Management |
| CVE-2014-0001 | y | n | y | n | n | Not Mitigated | Mitigated - Boundary Firewalls include anti-DOS |
| CVE-2014-0035 | n | n | y | n | n | Not Mitigated | Mitigated - Patch Management & SSL |
| CVE-2014-0160 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0207 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Management & SSL |
| CVE-2014-0232 | y | y | y | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2014-0259 | y | y | y | y | y | Not Mitigated | Mitigated - Malware Protection & Patch Management |
| CVE-2014-0266 | y | y | y | n | y | Not Mitigated | Partially Mitigated - Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2014-0294 | n | n | y | n | y | Not Mitigated | Mitigated - Secure Configuration, Anti-Malware |
| CVE-2014-0313 | y | n | y | y | n | Not Mitigated | Partially Mitigated - Secure Configuration (Secure Browser), Website Blacklisting |
| CVE-2014-0354 | y | n | n | y | n | Not Mitigated | Mitigated - Secure Configuration, Firmware Management |
| CVE-2014-0362 | y | y | y | y | n | Not Mitigated | Mitigated - Patch Management & Secure Configuration (Secure Browser & Web Hosting) |
| CVE-2014-0433 | y | y | y | n | y | Not Mitigated | Mitigated - Patch Management |
| CVE-2014-0488 | y | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Anti-Malware |
| CVE-2014-0493 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0494 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0498 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0515 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0533 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Access Control |
| CVE-2014-0536 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Access Control |
| CVE-2014-0562 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-0577 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Access Control |
| CVE-2014-0765 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2014-0767 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2014-0783 | n | n | n | n | n | Not Mitigated | Mitigated - Patch Managament, Secure Configuration (Port closing) |
| CVE-2014-1330 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Firewall, Website Blacklisting |
| CVE-2014-1342 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Firewall, Website Blacklisting |
| CVE-2014-1349 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Firewall, Access Control |
| CVE-2014-1356 | y | y | y | y | y | Not Mitigated | Mitigated - Secure Configuration, Malware Protection, Patch Management |
| CVE-2014-1370 | y | y | y | y | y | Not Mitigated | Mitigated - Malware Protection, Patch Management |
| CVE-2014-1379 | y | y | y | y | y | Not Mitigated | Mitigated - Malware Protection, Patch Management |
| CVE-2014-1379 | n | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Anti-Malware |
| CVE-2014-1382 | y | y | y | y | y | Not Mitigated | Mitigated - Website Blacklist, Patch Management |
| CVE-2014-1466 | y | n | n | n | y | Not Mitigated | Partially Mitigated - Patch Management |

| CVE | SME1 | SME2 | SME3 | SME4 | Idealised | No CE | With CE |
|---|---|---|---|---|---|---|---|
| CVE-2014-1472 | y | n | n | n | n | Not Mitigated | Mitigated - Website Blacklist, Patch Management |
| CVE-2014-1477 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1518 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1563 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1565 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1586 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1701 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-1740 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1744 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1753 | y | n | y | y | y | Not Mitigated | Mitigated - Website Blacklisting & Patch Management |
| CVE-2014-1806 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Managament |
| CVE-2014-1808 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall, Website Blacklisting & Patch Managament |
| CVE-2014-1811 | y | y | y | y | y | Not Mitigated | Mitigated - Firewall |
| CVE-2014-1812 | y | y | y | y | y | Not Mitigated | Mitigated - Strong Passwords (User Access) |
| CVE-2014-2014 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2014-2103 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall Anti DOS |
| CVE-2014-2109 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall & Patch Management |
| CVE-2014-2364 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-2416 | n | y | y | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-2554 | n | n | y | n | n | Not Mitigated | Mitigated - Patch Management, Access Control, Website Blacklisting |
| CVE-2014-2643 | n | y | n | n | n | Not Mitigated | Mitigated - Patch Management, Strong Passwords (User Access) |
| CVE-2014-2742 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall Anti DOS |
| CVE-2014-2768 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-2789 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-2791 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-2794 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-2808 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-2821 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-3444 | n | n | n | y | n | Not Mitigated | Mitigated - Anti-Malware, Patch Management |
| CVE-2014-3489 | n | n | n | n | n | Not Mitigated | Mitigated - Strong Passwords (User Access) |
| CVE-2014-3507 | n | n | y | y | y | Not Mitigated | Mitigated - Firewall & Patch Management |
| CVE-2014-3556 | y | n | y | n | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-3580 | y | y | y | n | n | Not Mitigated | Mitigated - Firewall Anti DOS, Patch Management |
| CVE-2014-3814 | n | n | n | n | n | Not Mitigated | Mitigated - Strong Passwords (User Access) |
| CVE-2014-3819 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall Anti-Dos, Firmware Updates |
| CVE-2014-3872 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration & Patch Management |
| CVE-2014-4044 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-4079 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4082 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4100 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4105 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4114 | y | y | y | y | n | Not Mitigated | Mitigated - Anti-Malware |
| CVE-2014-4127 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4130 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4132 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4133 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |

| CVE | SME1 | SME2 | SME3 | SME4 | Idealised | No CE | With CE |
|---|---|---|---|---|---|---|---|
| CVE-2014-4141 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-4481 | y | y | y | y | y | Not Mitigated | Mitigated - Patch Management, Anti-Malware |
| CVE-2014-4617 | y | y | n | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2014-4631 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Secure Configuration |
| CVE-2014-6040 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-6105 | n | n | n | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2014-6136 | n | n | n | n | n | Not Mitigated | Mitigated - Secure Configuration, Patch Management |
| CVE-2014-6363 | y | n | y | y | n | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-6369 | y | n | y | y |  | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-6378 | n | n | n | n | nn | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2014-6487 | n | n | y | n | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-7250 | n | y | y | n | n | Not Mitigated | Mitigated - Firewall, Patch Management |
| CVE-2014-7927 | y | y | y | y | n | Not Mitigated | Mitigated - Firewall, Secure Configuration (Access Control), Patch Management |
| CVE-2014-7945 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-8447 | y | y | y | y | n | Not Mitigated | Partially Mitigated - Anti-Malware, Patch Management |
| CVE-2014-8638 | y | y | y | y | y | Not Mitigated | Mitigated - Website Blacklisting, Secure Configuration (Secure Browser), Patch Management |
| CVE-2014-8835 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Patch Management |
| CVE-2014-9159 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Anti-Malware, Patch Management [Time Delay] |
| CVE-2014-9163 | y | y | y | y | y | Not Mitigated | Partially Mitigated - Anti-Malware, Patch Management [Time Delay] |
| CVE-2014-9350 | y | y | y | y | n | Not Mitigated | Mitigated - Firewall Anti-Dos, Firmware Updates |
| CVE-2014-9357 | n | n | n | n | n | Not Mitigated | Partially Mitigated - Patch Management, Anti-Malware, Secure Configuration |

# CVE Details

**CVE-2013-0008**
"win32k.sys in the kernel-mode drivers in Microsoft Windows Vista SP2,_x000D_ Windows Server 2008 SP2, R2, and R2 SP1, Windows 7 Gold and SP1,_x000D_ Windows 8, Windows Server 2012, and Windows RT does not properly_x000D_ handle window broadcast messages, which allows local users to gain_x000D_ privileges via a crafted application, aka ""Win32k Improper Message_x000D_ Handling Vulnerability."""

**CVE-2013-0022**
"Use-after-free vulnerability in Microsoft Internet Explorer 9 allows_x000D_ remote attackers to execute arbitrary code via a crafted web site that_x000D_ triggers access to a deleted object, aka ""Internet Explorer_x000D_ LsGetTrailInfo Use After Free Vulnerability."""

**CVE-2013-0084**
"Directory traversal vulnerability in Microsoft SharePoint Server 2010_x000D_ SP1 and SharePoint Foundation 2010 SP1 allows remote attackers to_x000D_ bypass intended read restrictions for content, and hijack user_x000D_ accounts, via a crafted URL, aka ""SharePoint Directory Traversal_x000D_ Vulnerability."""

**CVE-2013-0140**
SQL injection vulnerability in the Agent-Handler component in McAfee_x000D_ ePolicy Orchestrator (ePO) before 4.5.7 and 4.6.x before 4.6.6 allows_x000D_ remote attackers to execute arbitrary SQL commands via a crafted_x000D_ request over the Agent-Server communication channel.

**CVE-2013-0149**
The OSPF implementation in Cisco IOS 12.0 through 12.4 and 15.0_x000D_ through 15.3, IOS-XE 2.x through 3.9.xS, ASA and PIX 7.x through 9.1,_x000D_ FWSM, NX-OS, and StarOS before 14.0.50488 does not properly validate_x000D_ Link State Advertisement (LSA) type 1 packets before performing_x000D_ operations on the LSA database, which allows remote attackers to cause_x000D_ a denial of service (routing disruption) or obtain sensitive packet_x000D_ information via a (1) unicast or (2) multicast packet, aka Bug IDs_x000D_ CSCug34485, CSCug34469, CSCug39762, CSCug63304, and CSCug39795.

**CVE-2013-0172**
Samba 4.0.x before 4.0.1, in certain Active Directory_x000D_ domain-controller configurations, does not properly interpret Access_x000D_ Control Entries that are based on an objectClass, which allows remote_x000D_ authenticated users to bypass intended restrictions on modifying LDAP_x000D_ directory objects by leveraging (1) objectClass access by a user, (2)_x000D_ objectClass access by a group, or (3) write access to an attribute.

**CVE-2013-0174**
The external node classifier (ENC) API in Foreman before 1.1 allows_x000D_ remote attackers to obtain the hashed root password via an API_x000D_ request.

**CVE-2013-0199**
The default LDAP ACIs in FreeIPA 3.0 before 3.1.2 do not restrict_x000D_ access to the (1) ipaNTTrustAuthIncoming and (2)_x000D_ ipaNTTrustAuthOutgoing attributes, which allow remote attackers to_x000D_ obtain the Cross-Realm Kerberos Trust key via unspecified vectors.

**CVE-2013-0253**
The default configuration of Apache Maven 3.0.4, when using Maven_x000D_ Wagon 2.1, disables SSL certificate checks, which allows remote_x000D_ attackers to spoof servers via a man-in-the-middle (MITM) attack.

**CVE-2013-0270**
OpenStack Keystone Grizzly before 2013.1, Folsom, and possibly earlier_x000D_ allows remote attackers to cause a denial of service (CPU and memory_x000D_ consumption) via a large HTTP request, as demonstrated by a long_x000D_ tenant_name when requesting a token.

**CVE-2013-0481**
The console in IBM Sterling B2B Integrator 5.1 and 5.2 and Sterling File Gateway 2.1 and 2.2 allows remote attackers to read stack traces by triggering (1) an error or (2) an exception.

**CVE-2013-0598**
Cross-site request forgery (CSRF) vulnerability in the Web Client in_x000D_ IBM Rational ClearQuest 7.1 before 7.1.2.12, 8.0 before 8.0.0.8, and_x000D_ 8.0.1 before 8.0.1.1 allows remote attackers to hijack the_x000D_ authentication of arbitrary users.

**CVE-2013-0619**
Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and_x000D_ 11.x before 11.0.1 allow attackers to execute arbitrary code or cause_x000D_ a denial of service (memory corruption) via unspecified vectors, a_x000D_ different vulnerability than CVE-2012-1530, CVE-2013-0601,_x000D_ CVE-2013-0605, CVE-2013-0616, CVE-2013-0620, and CVE-2013-0623.

**CVE-2013-0633**
Buffer overflow in Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.

**CVE-2013-0649**
Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0644 and CVE-2013-1374.

**CVE-2013-0746**
Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x_x000D_ before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before_x000D_ 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 do not_x000D_ properly implement quickstubs that use the jsval data type for their_x000D_ return values, which allows remote attackers to execute arbitrary code_x000D_ or cause a denial of service (compartment mismatch and application_x000D_ crash) via crafted JavaScript code that is not properly handled during_x000D_ garbage collection.

**CVE-2013-0753**
Use-after-free vulnerability in the serializeToStream implementation_x000D_ in the XMLSerializer component in Mozilla Firefox before 18.0, Firefox_x000D_ ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before_x000D_ 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2,_x000D_ and SeaMonkey before 2.15 allows remote attackers to execute arbitrary_x000D_ code via crafted web content.

**CVE-2013-0787**
Use-after-free vulnerability in the nsEditor::IsPreformatted function_x000D_ in editor/libeditor/base/nsEditor.cpp in Mozilla Firefox before_x000D_ 19.0.2, Firefox ESR 17.x before 17.0.4, Thunderbird before 17.0.4,_x000D_ Thunderbird ESR 17.x before 17.0.4, and SeaMonkey before 2.16.1 allows_x000D_ remote attackers to execute arbitrary code via vectors involving an_x000D_ execCommand call.

**CVE-2013-0909**
The XSS Auditor in Google Chrome before 25.0.1364.152 allows remote attackers to obtain sensitive HTTP Referer information via unspecified vectors.

**CVE-2013-1035**
The iTunes ActiveX control in Apple iTunes before 11.1 allows remote_x000D_ attackers to execute arbitrary code or cause a denial of service_x000D_ (memory corruption) via a crafted web site.

**CVE-2013-1102**
The Wireless Intrusion Prevention System (wIPS) component on Cisco_x000D_ Wireless LAN Controller (WLC) devices with software 7.0 before_x000D_ 7.0.235.0, 7.1 and 7.2 before 7.2.110.0, and 7.3 before 7.3.101.0_x000D_ allows remote attackers to cause a denial of service (device reload)_x000D_ via crafted IP packets, aka Bug ID CSCtx80743.

**CVE-2013-1140**
The XML parser in Cisco Security Monitoring, Analysis, and Response_x000D_ System (MARS) allows remote attackers to read arbitrary files via an_x000D_ external entity declaration in conjunction with an entity reference,_x000D_ related to an XML External Entity (XXE) issue, aka Bug ID CSCue55093.

**CVE-2013-1144**
Memory leak in the IKEv1 implementation in Cisco IOS 15.1 allows_x000D_ remote attackers to cause a denial of service (memory consumption) via_x000D_ unspecified (1) IPv4 or (2) IPv6 IKE packets, aka Bug ID CSCth81055.

**CVE-2013-1153**
Cross-site request forgery (CSRF) vulnerability in the web interface_x000D_ in Cisco Prime Infrastructure allows remote attackers to hijack the_x000D_ authentication of arbitrary users, aka Bug ID CSCue84676.

**CVE-2013-1181**
Cisco NX-OS on Nexus 5500 devices 4.x and 5.x before 5.0(3)N2(2),_x000D_ Nexus 3000 devices 5.x before 5.0(3)U3(2), and Unified Computing_x000D_ System (UCS) 6200 devices before 2.0(1w) allows remote attackers to_x000D_ cause a denial of service (device reload) by sending a jumbo packet to_x000D_ the management interface, aka Bug IDs CSCtx17544, CSCts10593, and_x000D_ CSCtx95389.

**CVE-2013-1303**
"Use-after-free vulnerability in Microsoft Internet Explorer 6 through_x000D_ 10 allows remote attackers to execute arbitrary code via a crafted web_x000D_ site that triggers access to a deleted object, aka ""Internet Explorer_x000D_ Use After Free Vulnerability,"" a different vulnerability than_x000D_ CVE-2013-1304 and CVE-2013-1338."

**CVE-2013-1384**
Adobe Shockwave Player before 12.0.2.122 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-1386.

**CVE-2013-1388**
Unspecified vulnerability in Adobe ColdFusion 9.0 before Update 10,_x000D_ 9.0.1 before Update 9, 9.0.2 before Update 4, and 10 before Update 9_x000D_ allows attackers to obtain administrator-console access via unknown_x000D_ vectors.

**CVE-2013-1450**
Microsoft Internet Explorer 8 and 9, when the Proxy Settings_x000D_ configuration has the same Proxy address and Port values in the HTTP_x000D_ and Secure rows, does not properly reuse TCP sessions to the proxy_x000D_ server, which allows remote attackers to obtain sensitive information_x000D_ intended for a specific host via a crafted HTML document that triggers_x000D_ many HTTPS requests and then triggers an HTTP request to that host, as_x000D_ demonstrated by reading a Cookie header, aka MSRC 12096gd.

**CVE-2013-1472**
Unspecified vulnerability in the JavaFX component in Oracle Java SE_x000D_ JavaFX 2.2.4 and earlier allows remote attackers to affect_x000D_ confidentiality, integrity, and availability via unknown vectors, a_x000D_ different vulnerability than other CVEs listed in the February 2013_x000D_ CPU.

**CVE-2013-1553**
Unspecified vulnerability in the Oracle Web Services Manager component_x000D_ in Oracle Fusion Middleware 11.1.1.6.0 allows remote attackers to_x000D_ affect confidentiality and integrity via unknown vectors related to_x000D_ Web Services Security.

**CVE-2013-1620**
The TLS implementation in Mozilla Network Security Services (NSS) does_x000D_ not properly consider timing side-channel attacks on a noncompliant_x000D_ MAC check operation during the processing of malformed CBC padding,_x000D_ which allows remote attackers to conduct distinguishing attacks and_x000D_ plaintext-recovery attacks via statistical analysis of timing data for_x000D_ crafted packets, a related issue to CVE-2013-0169.

**CVE-2013-1627**
Absolute path traversal vulnerability in NTWebServer.exe in Indusoft_x000D_ Studio 7.0 and earlier and Advantech Studio 7.0 and earlier allows_x000D_ remote attackers to read arbitrary files via a full pathname in an_x000D_ argument to the sub_401A90 CreateFileW function.

**CVE-2013-1638**
Opera before 12.13 allows remote attackers to execute arbitrary code_x000D_ via crafted clipPaths in an SVG document.

**CVE-2013-1669**
Multiple unspecified vulnerabilities in the browser engine in Mozilla_x000D_ Firefox before 21.0 allow remote attackers to cause a denial of_x000D_ service (memory corruption and application crash) or possibly execute_x000D_ arbitrary code via unknown vectors.

**CVE-2013-1676**
The SelectionIterator::GetNextSegment function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.

**CVE-2013-1700**
The Mozilla Maintenance Service in Mozilla Firefox before 22.0 on_x000D_ Windows does not properly handle inability to launch the Mozilla_x000D_ Updater executable file, which allows local users to gain privileges_x000D_ via vectors involving placement of a Trojan horse executable file at_x000D_ an arbitrary location.

**CVE-2013-1734**
Cross-site request forgery (CSRF) vulnerability in attachment.cgi in_x000D_ Bugzilla 2.x, 3.x, and 4.0.x before 4.0.11; 4.1.x and 4.2.x before_x000D_ 4.2.7; and 4.3.x and 4.4.x before 4.4.1 allows remote attackers to_x000D_ hijack the authentication of arbitrary users for requests that commit_x000D_ an attachment change via an update action.

**CVE-2013-1777**
The JMX Remoting functionality in Apache Geronimo 3.x before 3.0.1, as_x000D_ used in IBM WebSphere Application Server (WAS) Community Edition_x000D_ 3.0.0.3 and other products, does not properly implement the RMI_x000D_ classloader, which allows remote attackers to execute arbitrary code_x000D_ by using the JMX connector to send a crafted serialized object.

**CVE-2013-2319**
FileMaker Pro before 12 and Pro Advanced before 12 does not verify_x000D_ X.509 certificates from SSL servers, which allows man-in-the-middle_x000D_ attackers to spoof servers and obtain sensitive information via a_x000D_ crafted certificate.

**CVE-2013-2340**
Unspecified vulnerability on the HP ProCurve JC###A, JC###B, JD###A, JD###B, JE###A, JF###A, JF###B, JF###C, JG###A, 658250-B21, and 658247-B21; HP 3COM routers and switches; and HP H3C routers and switches allows remote attackers to execute arbitrary code or obtain sensitive information via unknown vectors.

**CVE-2013-2350**
Unspecified vulnerability in HP Storage Data Protector 6.2X allows_x000D_ remote attackers to execute arbitrary code or cause a denial of_x000D_ service via unknown vectors, aka ZDI-CAN-1897.

**CVE-2013-2492**
Stack-based buffer overflow in Firebird 2.1.3 through 2.1.5 before_x000D_ 18514, and 2.5.1 through 2.5.3 before 26623, on Windows allows remote_x000D_ attackers to execute arbitrary code via a crafted packet to TCP port_x000D_ 3050, related to a missing size check during extraction of a group_x000D_ number from CNCT information.

**CVE-2013-2507**
Multiple cross-site scripting (XSS) vulnerabilities in the Brother MFC-9970CDW printer with firmware G (1.03) allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to admin/log_to_net.html or (2) kind parameter to fax/copy_settings.html, a different vulnerability than CVE-2013-2670 and CVE-2013-2671.

**CVE-2013-2736**
Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and_x000D_ 11.x before 11.0.03 allow attackers to execute arbitrary code or cause_x000D_ a denial of service (memory corruption) via unspecified vectors, a_x000D_ different vulnerability than CVE-2013-2718, CVE-2013-2719,_x000D_ CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723,_x000D_ CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732,_x000D_ CVE-2013-2734, CVE-2013-2735, CVE-2013-3337, CVE-2013-3338,_x000D_ CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.

**CVE-2013-2780**
Siemens SIMATIC S7-1200 PLCs 2.x and 3.x allow remote attackers to_x000D_ cause a denial of service (defect-mode transition and control outage)_x000D_ via crafted packets to UDP port 161 (aka the SNMP port).

**CVE-2013-2803**
ProSoft RadioLinx ControlScape before 6.00.040 uses a deficient PRNG_x000D_ algorithm and seeding strategy for passphrases, which makes it easier_x000D_ for remote attackers to obtain access via a brute-force attack.

**CVE-2013-2824**
Schneider Electric StruxureWare SCADA Expert Vijeo Citect 7.40, Vijeo_x000D_

Citect 7.20 through 7.30SP1, CitectSCADA 7.20 through 7.30SP1,_x000D_ StruxureWare PowerSCADA Expert 7.30 through 7.30SR1, and PowerLogic_x000D_ SCADA 7.20 through 7.20SR1 do not properly handle exceptions, which_x000D_ allows remote attackers to cause a denial of service via a crafted_x000D_ packet.

**CVE-2013-2826**
WellinTech KingSCADA before 3.1.2, KingAlarm&Event before 3.1, and_x000D_ KingGraphic before 3.1.2 perform authentication on the_x000D_ KAEClientManager console rather than on the server, which allows_x000D_ remote attackers to bypass intended access restrictions and discover_x000D_ credentials via a crafted packet to TCP port 8130.

**CVE-2013-2920**
The DoResolveRelativeHost function in url/url_canon_relative.cc in_x000D_ Google Chrome before 30.0.1599.66 allows remote attackers to cause a_x000D_ denial of service (out-of-bounds read) via a relative URL containing a_x000D_ hostname, as demonstrated by a protocol-relative URL beginning with a_x000D_ //www.google.com/ substring.

**CVE-2013-3064**
Open redirect vulnerability in ui/dynamic/unsecured.html in Linksys_x000D_ EA6500 with firmware 1.1.28.147876 allows remote attackers to redirect_x000D_ users to arbitrary web sites and conduct phishing attacks via a URL in_x000D_ the target parameter.

**CVE-2013-3116**
"Microsoft Internet Explorer 7 through 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2013-3137**
"Microsoft FrontPage 2003 SP3 does not properly parse DTDs, which allows remote attackers to obtain sensitive information via crafted XML data in a FrontPage document, aka ""XML Disclosure Vulnerability."""

**CVE-2013-3194**
"Microsoft Internet Explorer 9 allows remote attackers to execute_x000D_ arbitrary code or cause a denial of service (memory corruption) via a_x000D_ crafted web site, aka ""Internet Explorer Memory Corruption_x000D_ Vulnerability."""

**CVE-2013-3199**
"Microsoft Internet Explorer 6 through 10 allows remote attackers to_x000D_ execute arbitrary code or cause a denial of service (memory_x000D_ corruption) via a crafted web site, aka ""Internet Explorer Memory_x000D_ Corruption Vulnerability."""

**CVE-2013-3201**
"Microsoft Internet Explorer 9 and 10 allows remote attackers to_x000D_ execute arbitrary code or cause a denial of service (memory_x000D_ corruption) via a crafted web site, aka ""Internet Explorer Memory_x000D_ Corruption Vulnerability,"" a different vulnerability than_x000D_ CVE-2013-3203, CVE-2013-3206, CVE-2013-3207, and CVE-2013-3209."

**CVE-2013-3206**
"Microsoft Internet Explorer 9 and 10 allows remote attackers to_x000D_ execute arbitrary code or cause a denial of service (memory_x000D_ corruption) via a crafted web site, aka ""Internet Explorer Memory_x000D_ Corruption Vulnerability,"" a different vulnerability than_x000D_ CVE-2013-3201, CVE-2013-3203, CVE-2013-3207, and CVE-2013-3209."

**CVE-2013-3280**
EMC RSA Authentication Agent 7.1.x before 7.1.2 for Web for Internet_x000D_ Information Services has a fail-open design, which allows remote_x000D_ attackers to bypass intended access restrictions via vectors that_x000D_ trigger an agent crash.

**CVE-2013-3387**
Cisco Prime Central for Hosted Collaboration Solution (HCS) Assurance_x000D_ 8.6 and 9.x before 9.2(1) allows remote attackers to cause a denial of_x000D_ service (disk consumption) via a flood of TCP packets to port 5400,_x000D_ leading to large error-log files, aka Bug ID CSCua42724.

**CVE-2013-3417**
The administrative web interface in Cisco Video Surveillance Operations Manager does not properly perform authentication, which allows remote attackers to watch video feeds via a crafted URL, aka Bug ID CSCtg72262.

**CVE-2013-3632**
The Cron service in rpc.php in OpenMediaVault allows remote_x000D_ authenticated users to execute cron jobs as arbitrary users and_x000D_ execute arbitrary commands via the username parameter.

**CVE-2013-3656**
Cybozu Office 9.1.0 and earlier does not properly manage sessions,_x000D_ which allows remote attackers to bypass authentication by leveraging_x000D_ knowledge of a login URL.

**CVE-2013-3856**
"Microsoft Word 2003 SP3 and Word Viewer allow remote attackers to_x000D_ execute arbitrary code or cause a denial of service (memory_x000D_ corruption) via a crafted Office document, aka ""Word Memory Corruption_x000D_ Vulnerability."""

**CVE-2013-3860**
"Microsoft .NET Framework 2.0 SP2, 3.5, 3.5 SP1, 3.5.1, 4, and 4.5 does_x000D_ not properly parse a DTD during XML digital-signature validation,_x000D_ which allows remote attackers to cause a denial of service_x000D_ (application crash or hang) via a crafted signed XML document, aka_x000D_ ""Entity Expansion Vulnerability."""

**CVE-2013-3893**
Use-after-free vulnerability in the SetMouseCapture implementation in_x000D_ mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote_x000D_ attackers to execute arbitrary code via crafted JavaScript strings, as_x000D_ demonstrated by use of an ms-help: URL that triggers loading of_x000D_ hxds.dll.

**CVE-2013-3897**
"Use-after-free vulnerability in the CDisplayPointer class in mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted JavaScript code that uses the onpropertychange event handler, as exploited in the wild in September and October 2013, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2013-3900**
"The WinVerifyTrust function in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate PE file digests during Authenticode signature verification, which allows remote attackers to execute arbitrary code via a crafted PE file, aka ""WinVerifyTrust Signature Validation Vulnerability."""

**CVE-2013-3905**
"Microsoft Outlook 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT does_x000D_ not properly expand metadata contained in S/MIME certificates, which_x000D_ allows remote attackers to obtain sensitive network configuration and_x000D_ state information via a crafted certificate in an e-mail message, aka_x000D_ ""S/MIME AIA Vulnerability."""

**CVE-2013-4223**
The Gentoo Nullmailer package before 1.11-r2 uses world-readable_x000D_ permissions for /etc/nullmailer/remotes, which allows local users to_x000D_ obtain SMTP authentication credentials by reading the file.

**CVE-2013-4436**
The default configuration for salt-ssh in Salt (aka SaltStack) 0.17.0_x000D_ does not validate the SSH host key of requests, which allows remote_x000D_ attackers to have unspecified impact via a man-in-the-middle (MITM)_x000D_ attack.

**CVE-2013-4478**
Sup before 0.13.2.1 and 0.14.x before 0.14.1.1 allows remote attackers_x000D_ to execute arbitrary commands via shell metacharacters in the filename_x000D_ of an email attachment.

**CVE-2013-4529**
Buffer overflow in hw/pci/pcie_aer.c in QEMU before 1.7.2 allows_x000D_ remote attackers to cause a denial of service and possibly execute_x000D_ arbitrary code via a large log_num value in a savevm image.

**CVE-2013-4555**
Cross-site request forgery (CSRF) vulnerability in_x000D_ ecrire/action/logout.php in SPIP before 2.1.24 allows remote attackers_x000D_ to hijack the authentication of arbitrary users for requests that_x000D_ logout the user via unspecified vectors.

**CVE-2013-4776**
NETGEAR ProSafe GS724Tv3 and GS716Tv2 with firmware 5.4.1.13 and_x000D_ earlier, GS748Tv4 5.4.1.14, and GS510TP 5.0.4.4 allows remote_x000D_ attackers to cause a denial of service (reboot or crash) via a crafted_x000D_ HTTP request to filesystem/.

**CVE-2013-4782**

The Supermicro BMC implementation allows remote attackers to bypass_x000D_ authentication and execute arbitrary IPMI commands by using cipher_x000D_ suite 0 (aka cipher zero) and an arbitrary password.

**CVE-2013-5057**
"hxds.dll in Microsoft Office 2007 SP3 and 2010 SP1 and SP2 does not implement the ASLR protection mechanism, which makes it easier for remote attackers to execute arbitrary code via a crafted COM component on a web site that is visited with Internet Explorer, as exploited in the wild in December 2013, aka ""HXDS ASLR Vulnerability."""

**CVE-2013-5369**
IBM SPSS Analytical Decision Management 6.1 before IF1, 6.2 before_x000D_ IF1, and 7.0 before FP1 IF6 might allow remote attackers to execute_x000D_ arbitrary code by deploying and accessing a service.

**CVE-2013-5428**
IBM WebSphere DataPower XC10 appliances 2.5.0 do not require_x000D_ authentication for all administrative actions, which allows remote_x000D_ attackers to cause a denial of service via unspecified vectors.

**CVE-2013-5431**
Open redirect vulnerability in IBM Tivoli Federated Identity Manager_x000D_ (TFIM) 6.1.1 before IF 15, 6.2.0 before IF 14, 6.2.1, and 6.2.2 before_x000D_ IF 8 and Tivoli Federated Identity Manager Business Gateway (TFIMBG)_x000D_ 6.1.1 before IF 15, 6.2.0 before IF 14, 6.2.1, and 6.2.2 before IF 8_x000D_ allows remote attackers to redirect users to arbitrary web sites and_x000D_ conduct phishing attacks via unspecified vectors.

**CVE-2013-5494**
Cross-site request forgery (CSRF) vulnerability in the web framework_x000D_ in Cisco Unified MeetingPlace Solution, as used in Unified_x000D_ MeetingPlace Web Conferencing and Unified MeetingPlace, allows remote_x000D_ attackers to hijack the authentication of arbitrary users, aka Bug IDs_x000D_ CSCui45209 and CSCui44674.

**CVE-2013-5507**
The IPsec implementation in Cisco Adaptive Security Appliance (ASA)_x000D_ Software 9.1 before 9.1(1.7), when an IPsec VPN tunnel is enabled,_x000D_ allows remote attackers to cause a denial of service (device reload)_x000D_ via a (1) ICMP or (2) ICMPv6 packet that is improperly handled during_x000D_ decryption, aka Bug ID CSCue18975.

**CVE-2013-5536**
Cisco Secure Access Control System (ACS) does not properly implement_x000D_ an incoming-packet firewall rule, which allows remote attackers to_x000D_ cause a denial of service (process crash) via a flood of crafted_x000D_ packets, aka Bug ID CSCui51521.

**CVE-2013-5559**
Buffer overflow in the Active Template Library (ATL) framework in the_x000D_ VPNAPI COM module in Cisco AnyConnect Secure Mobility Client 2.x_x000D_ allows user-assisted remote attackers to execute arbitrary code via a_x000D_ crafted HTML document, aka Bug ID CSCuj58139.

**CVE-2013-5561**
The Safe Search enforcement feature in Cisco Adaptive Security_x000D_ Appliance (ASA) CX Context-Aware Security Software does not properly_x000D_ perform filtering, which allows remote attackers to bypass intended_x000D_ policy restrictions via unspecified vectors, aka Bug ID CSCui94622.

**CVE-2013-5751**
Directory traversal vulnerability in SAP NetWeaver 7.x allows remote_x000D_ attackers to read arbitrary files via unspecified vectors.

**CVE-2013-5757**
Absolute path traversal vulnerability in Yealink VoIP Phone SIP-T38G allows remote authenticated users to read arbitrary files via a full pathname in the dumpConfigFile function in the command parameter to cgi-bin/cgiServer.exx.

**CVE-2013-5828**
Unspecified vulnerability in the Enterprise Manager Base Platform_x000D_ component in Oracle Enterprise Manager Grid Control EM Base Platform_x000D_ 10.2.0.5 and 11.1.0.1; EM DB Control 11.1.0.7, 11.2.0.2, and 11.2.0.3;_x000D_ and EM Plugin for DB 12.1.0.2 and 12.1.0.3 allows remote attackers to_x000D_ affect integrity via unknown vectors related to Storage Management.

**CVE-2013-6167**
Mozilla Firefox through 27 sends HTTP Cookie headers without first_x000D_ validating that they have the required character-set restrictions,_x000D_ which allows remote attackers to conduct the equivalent of a_x000D_ persistent Logout CSRF attack via a crafted parameter that forces a_x000D_ web application to set a malformed cookie within an HTTP response.

**CVE-2013-6188**
Cross-site request forgery (CSRF) vulnerability in HP System_x000D_ Management Homepage (SMH) 7.1 through 7.2.2 allows remote attackers to_x000D_ hijack the authentication of unspecified victims via unknown vectors.

**CVE-2013-6284**
"Unspecified vulnerability in the Statutory Reporting for Insurance_x000D_ (FS_SR) component in the Financial Services module for SAP ERP Central_x000D_ Component (ECC) allows attackers to execute arbitrary code via_x000D_ unspecified vectors, related to a ""code injection vulnerability."""

**CVE-2013-6396**
The OpenStack Python client library for Swift (python-swiftclient) 1.0_x000D_ through 1.9.0 does not verify X.509 certificates from SSL servers,_x000D_ which allows man-in-the-middle attackers to spoof servers and obtain_x000D_ sensitive information via a crafted certificate.

**CVE-2013-6475**
Multiple integer overflows in (1) OPVPOutputDev.cxx and (2)_x000D_ oprs/OPVPSplash.cxx in the pdftoopvp filter in CUPS and cups-filters_x000D_ before 1.0.47 allow remote attackers to execute arbitrary code via a_x000D_ crafted PDF file, which triggers a heap-based buffer overflow.

**CVE-2013-6660**
The drag-and-drop implementation in Google Chrome before 33.0.1750.117 does not properly restrict the information in WebDropData data structures, which allows remote attackers to discover full pathnames via a crafted web site.

**CVE-2013-6699**
The Control and Provisioning of Wireless Access Points (CAPWAP)_x000D_ protocol implementation on Cisco Wireless LAN Controller (WLC) devices_x000D_ allows remote attackers to cause a denial of service via a crafted_x000D_ CAPWAP packet that triggers a buffer over-read, aka Bug ID CSCuh81880.

**CVE-2013-6702**
The management implementation on Cisco ONS 15454 controller cards with_x000D_ software 9.8 and earlier allows remote attackers to cause a denial of_x000D_ service (card reset) via crafted packets, aka Bug ID CSCtz50902.

**CVE-2013-6979**
The VTY authentication implementation in Cisco IOS XE 03.02.xxSE and 03.03.xxSE incorrectly relies on the Linux-IOS internal-network configuration, which allows remote attackers to bypass authentication by leveraging access to a 192.168.x.2 source IP address, aka Bug ID CSCuj90227.

**CVE-2013-6994**
OpenText Exceed OnDemand (EoD) 8 transmits the session ID in_x000D_ cleartext, which allows remote attackers to perform session fixation_x000D_ attacks by sniffing the network.

**CVE-2013-7004**
D-Link DSR-150 with firmware before 1.08B44; DSR-150N with firmware before 1.05B64; DSR-250 and DSR-250N with firmware before 1.08B44; and DSR-500, DSR-500N, DSR-1000, and DSR-1000N with firmware before 1.08B77 have a hardcoded account of username gkJ9232xXyruTRmY, which makes it easier for remote attackers to obtain access by leveraging knowledge of the username.

**CVE-2013-7043**
Multiple cross-site request forgery (CSRF) vulnerabilities on Cisco_x000D_ Scientific Atlanta DPR2320R2 routers with software 2.0.2r1262-090417_x000D_ allow remote attackers to hijack the authentication of administrators_x000D_ for requests that (1) change a password via the Password parameter to_x000D_ goform/RgSecurity; (2) reboot the device via the Restart parameter to_x000D_ goform/restart; (3) modify Wi-Fi settings, as demonstrated by the_x000D_ WpaPreSharedKey parameter to goform/wlanSecurity; or (4) modify_x000D_ parental controls via the ParentalPassword parameter to_x000D_ goform/RgParentalBasic.

**CVE-2013-7389**
Multiple cross-site scripting (XSS) vulnerabilities in D-Link DIR-645 Router (Rev. A1) with firmware before 1.04B11 allow remote attackers to inject arbitrary web script or HTML via the (1) deviceid parameter to parentalcontrols/bind.php, (2) RESULT parameter to info.php, or (3) receiver parameter to bsc_sms_send.php.

**CVE-2014-0001**
Buffer overflow in client/mysql.cc in Oracle

MySQL and MariaDB before 5.5.35 allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary code via a long server version string.

**CVE-2014-0035**
The SymmetricBinding in Apache CXF before 2.6.13 and 2.7.x before 2.7.10, when EncryptBeforeSigning is enabled and the UsernameToken policy is set to an EncryptedSupportingToken, transmits the UsernameToken in cleartext, which allows remote attackers to obtain sensitive information by sniffing the network.

**CVE-2014-0160**
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

**CVE-2014-0207**
The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.

**CVE-2014-0259**
"Microsoft Word 2007 SP3 and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka ""Word Memory Corruption Vulnerability."""

**CVE-2014-0266**
"The XMLHTTP ActiveX controls in XML Core Services 3.0 in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to bypass the Same Origin Policy via a web page that is visited in Internet Explorer, aka ""MSXML Information Disclosure Vulnerability."""

**CVE-2014-0294**
"Microsoft Forefront Protection 2010 for Exchange Server does not properly parse e-mail content, which might allow remote attackers to execute arbitrary code via a crafted message, aka ""RCE Vulnerability."""

**CVE-2014-0313**
"Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-0321."

**CVE-2014-0354**
The ZyXEL Wireless N300 NetUSB NBG-419N router with firmware 1.00(BFQ.6)C0 has a hardcoded password of qweasdzxc for an unspecified account, which allows remote attackers to obtain index.asp login access via an HTTP request.

**CVE-2014-0362**
Cross-site scripting (XSS) vulnerability on Google Search Appliance (GSA) devices before 7.0.14.G.216 and 7.2 before 7.2.0.G.114, when dynamic navigation is configured, allows remote attackers to inject arbitrary web script or HTML via input included in a SCRIPT element.

**CVE-2014-0433**
Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote attackers to affect availability via unknown vectors related to Thread Pooling.

**CVE-2014-0488**
"APT before 1.0.9 does not ""invalidate repository data"" when moving from an unauthenticated to authenticated state, which allows remote attackers to have unspecified impact via crafted repository data."

**CVE-2014-0493**
Adobe Reader and Acrobat 10.x before 10.1.9 and 11.x before 11.0.06 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0495.

**CVE-2014-0494**
Adobe Digital Editions 2.0.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.

**CVE-2014-0498**
Stack-based buffer overflow in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows attackers to execute arbitrary code via unspecified vectors.

**CVE-2014-0515**
Buffer overflow in Adobe Flash Player before 11.7.700.279 and 11.8.x through 13.0.x before 13.0.0.206 on Windows and OS X, and before 11.2.202.356 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in April 2014.

**CVE-2014-0533**
Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0532.

**CVE-2014-0536**
Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

**CVE-2014-0562**
"Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 10.x before 10.1.12 and 11.x before 11.0.09 on OS X allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka ""Universal XSS (UXSS)."""

**CVE-2014-0577**
"Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified ""type confusion,"" a different vulnerability than CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, and CVE-2014-0590."

**CVE-2014-0765**
Stack-based buffer overflow in Advantech WebAccess before 7.2 allows remote attackers to execute arbitrary code via a long GotoCmd argument.

**CVE-2014-0767**
Stack-based buffer overflow in Advantech WebAccess before 7.2 allows remote attackers to execute arbitrary code via a long AccessCode argument.

**CVE-2014-0783**
Stack-based buffer overflow in BKHOdeq.exe in Yokogawa CENTUM CS 3000 R3.09.50 and earlier allows remote attackers to execute arbitrary code via a crafted TCP packet.

**CVE-2014-1330**
WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.

**CVE-2014-1342**
WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.

**CVE-2014-1349**
Use-after-free vulnerability in Safari in Apple iOS before 7.1.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an invalid URL.

**CVE-2014-1356**
Heap-based buffer overflow in launchd in Apple iOS before 7.1.2, Apple OS X before 10.9.4, and Apple TV before 6.1.2 allows attackers to execute arbitrary code via a crafted application that sends IPC messages.

**CVE-2014-1370**
The byte-swapping implementation in copyfile in Apple OS X before 10.9.4 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds memory access and application crash) via a crafted AppleDouble file in a ZIP archive.

**CVE-2014-1379**
Graphics Drivers in Apple OS X before 10.9.4 allows attackers to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via a 32-bit

executable file for a crafted application.

**CVE-2014-1382**
WebKit, as used in Apple iOS before 7.1.2, Apple Safari before 6.1.5 and 7.x before 7.0.5, and Apple TV before 6.1.2, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-06-30-1, APPLE-SA-2014-06-30-3, and APPLE-SA-2014-06-30-4.

**CVE-2014-1466**
SQL injection vulnerability in CSP MySQL User Manager 2.3 allows remote attackers to execute arbitrary SQL commands via the login field of the login page.

**CVE-2014-1472**
Multiple cross-site scripting (XSS) vulnerabilities in the Enterprise Manager in McAfee Vulnerability Manager (MVM) 7.5.5 and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

**CVE-2014-1477**
Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 27.0, Firefox ESR 24.x before 24.3, Thunderbird before 24.3, and SeaMonkey before 2.24 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

**CVE-2014-1518**
Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 29.0, Firefox ESR 24.x before 24.5, Thunderbird before 24.5, and SeaMonkey before 2.26 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.

**CVE-2014-1563**
Use-after-free vulnerability in the mozilla::DOMSVGLength::GetTearOff function in Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an SVG animation with DOM interaction that triggers incorrect cycle collection.

**CVE-2014-1565**
The mozilla::dom::AudioEventTimeline function in the Web Audio API implementation in Mozilla Firefox before 32.0, Firefox ESR 31.x before 31.1, and Thunderbird 31.x before 31.1 does not properly create audio timelines, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted API calls.

**CVE-2014-1586**
content/base/src/nsDocument.cpp in Mozilla Firefox before 33.0, Firefox ESR 31.x before 31.2, and Thunderbird 31.x before 31.2 does not consider whether WebRTC video sharing is occurring, which allows remote attackers to obtain sensitive information from the local camera in certain IFRAME situations by maintaining a session after the user temporarily navigates away.

**CVE-2014-1701**
The GenerateFunction function in bindings/scripts/code_generator_v8.pm in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the EventTarget::dispatchEvent function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.

**CVE-2014-1740**
Multiple use-after-free vulnerabilities in net/websockets/websocket_job.cc in the WebSockets implementation in Google Chrome before 34.0.1847.137 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to WebSocketJob deletion.

**CVE-2014-1744**
Integer overflow in the AudioInputRenderer Host::OnCreateStream function in content/browser/renderer host/media/audio input_renderer_host.cc in Google Chrome before 35.0.1916.114 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large shared-memory allocation.

**CVE-2014-1753**
"Microsoft Internet Explorer 6 through 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-1806**
"The .NET Remoting implementation in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, and 4.5.1 does not properly restrict memory access, which allows remote attackers to execute arbitrary code via vectors involving malformed objects, aka ""TypeFilterLevel Vulnerability."""

**CVE-2014-1808**
"Microsoft Office 2013 Gold, SP1, RT, and RT SP1 allows remote attackers to obtain sensitive token information via a web site that sends a crafted response during opening of an Office document, aka ""Token Reuse Vulnerability."""

**CVE-2014-1811**
"The TCP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to cause a denial of service (non-paged pool memory consumption and system hang) via malformed data in the Options field of a TCP header, aka ""TCP Denial of Service Vulnerability."""

**CVE-2014-1812**
"The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka ""Group Policy Preferences Password Elevation of Privilege Vulnerability."""

**CVE-2014-2014**
imapsync before 1.584, when running with the –tls option, attempts a cleartext login when a certificate verification failure occurs, which allows remote attackers to obtain credentials by sniffing the network.

**CVE-2014-2103**
Cisco Intrusion Prevention System (IPS) Software allows remote attackers to cause a denial of service (MainApp process outage) via malformed SNMP packets, aka Bug IDs CSCum52355 and CSCul49309.

**CVE-2014-2109**
The TCP Input module in Cisco IOS 12.2 through 12.4 and 15.0 through 15.4, when NAT is used, allows remote attackers to cause a denial of service (memory consumption or device reload) via crafted TCP packets, aka Bug IDs CSCuh33843 and CSCuj41494.

**CVE-2014-2364**
Multiple stack-based buffer overflows in Advantech WebAccess before 7.2 allow remote attackers to execute arbitrary code via a long string in the (1) ProjectName, (2) SetParameter, (3) NodeName, (4) CCDParameter, (5) SetColor, (6) AlarmImage, (7) GetParameter, (8) GetColor, (9) ServerResponse, (10) SetBaud, or (11) IPAddress parameter to an ActiveX control in (a) webvact.ocx, (b) dvs.ocx, or (c) webdact.ocx.

**CVE-2014-2416**
Unspecified vulnerability in the Oracle Data Integrator component in Oracle Fusion Middleware 11.1.1.3.0 allows remote attackers to affect availability via unknown vectors related to Data Quality, a different vulnerability than CVE-2014-2407, CVE-2014-2415, CVE-2014-2417, and CVE-2014-2418.

**CVE-2014-2554**
OTRS 3.1.x before 3.1.21, 3.2.x before 3.2.16, and 3.3.x before 3.3.6 allows remote attackers to conduct clickjacking attacks via an IFRAME element.

**CVE-2014-2643**
Unspecified vulnerability in HP Systems Insight Manager (SIM) before 7.4 allows remote authenticated users to gain privileges via unknown vectors.

**CVE-2014-2742**
"Isode M-Link before 16.0v7 does not properly restrict the processing of compressed XML elements, which allows remote attackers to cause a denial of service (resource consumption) via a crafted XMPP stream, aka an ""xmppbomb"" attack."

**CVE-2014-2768**
"Microsoft Internet Explorer 6 through 8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2773."

**CVE-2014-2789**
"Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2795, CVE-2014-2798, and CVE-2014-2804."

**CVE-2014-2791**
"Microsoft Internet Explorer 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-2794**
"Microsoft Internet Explorer 6 and 7 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2788."

**CVE-2014-2808**
"Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2796, CVE-2014-2825, CVE-2014-4050, CVE-2014-4055, and CVE-2014-4067."

**CVE-2014-2821**
"Microsoft Internet Explorer 8 and 9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-3444**
The GetGUID function in codecs/dmp4.dll in RealNetworks RealPlayer 16.0.3.51 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (write access violation and application crash) via a malformed .3gp file.

**CVE-2014-3489**
lib/util/miq-password.rb in Red Hat CloudForms 3.0 Management Engine (CFME) before 5.2.4.2 uses a hard-coded salt, which makes it easier for remote attackers to guess passwords via a brute force attack.

**CVE-2014-3507**
Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

**CVE-2014-3556**
"The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a ""plaintext command injection"" attack, a similar issue to CVE-2011-0411."

**CVE-2014-3580**
The mod_dav_svn Apache HTTPD server module in Apache Subversion 1.x before 1.7.19 and 1.8.x before 1.8.11 allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a REPORT request for a resource that does not exist.

**CVE-2014-3814**
The Juniper Networks NetScreen Firewall devices with ScreenOS before 6.3r17, when configured to use the internal DNS lookup client, allows remote attackers to cause a denial of service (crash and reboot) via a sequence of malformed packets to the device IP.

**CVE-2014-3819**
Juniper Junos 11.4 before 11.4R12, 12.1 before 12.1R10, 12.1X44 before 12.1X44-D35, 12.1X45 before 12.1X45-D25, 12.1X46 before 12.1X46-D20, 12.1X47 before 12.1X47-D10, 12.2 before 12.2R8, 12.3 before 12.3R7, 13.1 before 13.1R4, 13.2 before 13.2R4, 13.3 before 13.3R2, and 14.1 before 14.1R1, when Auto-RP is enabled, allows remote attackers to cause a denial of service (RDP routing process crash and restart) via a malformed PIM packet.

**CVE-2014-3872**
Multiple SQL injection vulnerabilities in the administration login page in D-Link DAP-1350 (Rev. A1) with firmware 1.14 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password.

**CVE-2014-4044**
OpenAFS 1.6.8 does not properly clear the fields in the host structure, which allows remote attackers to cause a denial of service (uninitialized memory access and crash) via unspecified vectors related to TMAY requests.

**CVE-2014-4079**
"Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111."

**CVE-2014-4082**
"Microsoft Internet Explorer 6 through 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-4100**
"Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111."

**CVE-2014-4105**
"Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079, CVE-2014-4081, CVE-2014-4083, CVE-2014-4085, CVE-2014-4088, CVE-2014-4090, CVE-2014-4094, CVE-2014-4097, CVE-2014-4100, CVE-2014-4103, CVE-2014-4104, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, and CVE-2014-4111."

**CVE-2014-4114**
"Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a ""Sandworm"" attack in June through October 2014, aka ""Windows OLE Remote Code Execution Vulnerability."""

**CVE-2014-4127**
"Microsoft Internet Explorer 6 through 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-4130**
"Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-4132 and CVE-2014-4138."

**CVE-2014-4132**
"Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-4130 and CVE-2014-4138."

**CVE-2014-4133**
"Microsoft Internet Explorer 6 and 7 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability,"" a different vulnerability than CVE-2014-4137."

**CVE-2014-4141**
"Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-4481**
Integer overflow in CoreGraphics in Apple iOS before 8.1.3, Apple OS X before 10.10.2, and Apple TV before 7.0.3 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF document.

**CVE-2014-4617**
The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-dependent attackers to cause a denial of service (infinite loop) via malformed compressed packets, as demonstrated by

an a3 01 5b ff byte sequence.

**CVE-2014-4631**
RSA Adaptive Authentication (On-Premise) 6.0.2.1 through 7.1 P3, when using device binding in a Challenge SOAP call or using the RSA Adaptive Authentication Integration Adapters with Out-of-Band Phone (Authentify) functionality, conducts permanent device binding even when authentication fails, which allows remote attackers to bypass authentication.

**CVE-2014-5528**
The Appsflyer library for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

**CVE-2014-6040**
"GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of ""0xffff"" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8."

**CVE-2014-6105**
IBM Security Identity Manager 6.x before 6.0.0.3 IF14 allows remote attackers to conduct clickjacking attacks via unspecified vectors.

**CVE-2014-6136**
IBM Security AppScan Standard 8.x and 9.x before 9.0.1.1 FP1 supports unencrypted sessions, which allows remote attackers to obtain sensitive information by sniffing the network.

**CVE-2014-6164**
IBM WebSphere Application Server 8.0.x before 8.0.0.10 and 8.5.x before 8.5.5.4 allows remote attackers to spoof OpenID and OpenID Connect cookies, and consequently obtain sensitive information, via a crafted URL.

**CVE-2014-6363**
"vbscript.dll in Microsoft VBScript 5.6 through 5.8, as used with Internet Explorer 6 through 11 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""VBScript Memory Corruption Vulnerability."""

**CVE-2014-6369**
"Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka ""Internet Explorer Memory Corruption Vulnerability."""

**CVE-2014-6378**
Juniper Junos 11.4 before R12-S4, 12.1X44 before D35, 12.1X45 before D30, 12.1X46 before D25, 12.1X47 before D10, 12.2 before R9, 12.2X50 before D70, 12.3 before R7, 13.1 before R4 before S3, 13.1X49 before D55, 13.1X50 before D30, 13.2 before R5, 13.2X50 before D20, 13.2X51 before D26 and D30, 13.2X52 before D15, 13.3 before R3, and 14.1 before R1 allows remote attackers to cause a denial of service (router protocol daemon crash) via a crafted RSVP PATH message.

**CVE-2014-6487**
Unspecified vulnerability in the Oracle Identity Manager component in Oracle Fusion Middleware 11.1.1.5, 11.1.1.7, 11.1.2.1, and 11.1.2.2 allows remote authenticated users to affect integrity via unknown vectors related to End User Self Service.

**CVE-2014-7250**
The TCP stack in 4.3BSD Net/2, as used in FreeBSD 5.4, NetBSD possibly 2.0, and OpenBSD possibly 3.6, does not properly implement the session timer, which allows remote attackers to cause a denial of service (resource consumption) via crafted packets.

**CVE-2014-7927**
The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.

**CVE-2014-7945**
OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.

**CVE-2014-8447**
Adobe Reader and Acrobat 10.x before 10.1.13 and 11.x before 11.0.10 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-8445, CVE-2014-8446, CVE-2014-8456, CVE-2014-8458, CVE-2014-8459, CVE-2014-8461, and CVE-2014-9158.

**CVE-2014-8638**
The navigator.sendBeacon implementation in Mozilla Firefox before 35.0, Firefox ESR 31.x before 31.4, Thunderbird before 31.4, and SeaMonkey before 2.32 omits the CORS Origin header, which allows remote attackers to bypass intended CORS access-control checks and conduct cross-site request forgery (CSRF) attacks via a crafted web site.

**CVE-2014-8835**
"The xpc_data_get_bytes function in libxpc in Apple OS X before 10.10.2 does not verify that a dictionary's Attributes key has the xpc_data data type, which allows attackers to execute arbitrary code by providing a crafted dictionary to sysmond, related to an ""XPC type confusion"" issue."

**CVE-2014-9159**
Heap-based buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.13 and 11.x before 11.0.10 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-8457 and CVE-2014-8460.

**CVE-2014-9163**
Stack-based buffer overflow in Adobe Flash Player before 13.0.0.259 and 14.x and 15.x before 15.0.0.246 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in December 2014.

**CVE-2014-9350**
"TP-Link TL-WR740N 4 with firmware 3.17.0 Build 140520, 3.16.6 Build 130529, and 3.16.4 Build 130205 allows remote attackers to cause a denial of service (httpd crash) via vectors involving a ""new"" value in the isNew parameter to PingIframeRpm.htm."

**CVE-2014-9357**
Docker 1.3.2 allows remote attackers to execute arbitrary code with root privileges via a crafted (1) image or (2) build in a Dockerfile in an LZMA (.xz) archive, related to the chroot for archive extraction.

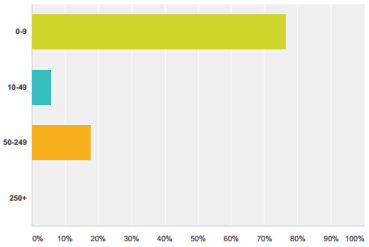
# Survey Responses

**Q1 Please enter your organisational email (i.e. j.doe@company.co.uk) to qualify for the raffle**

Answered: 12 Skipped: 5

**Q2 How many computer workstations are located on-site?**

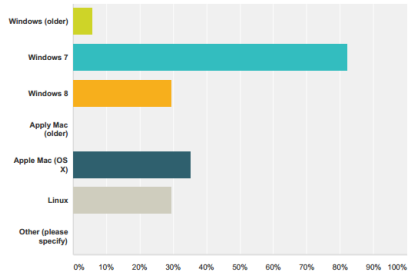
Answered: 17 Skipped: 0




| Answer Choices | Responses | |
|---|---|---|
| 0-9 | 76.47% | 13 |
| 10-49 | 5.88% | 1 |
| 50-249 | 17.65% | 3 |
| 250+ | 0.00% | 0 |
| Total | | 17 |

**Q3 Which Operating Systems are in use for workstations on-site?**

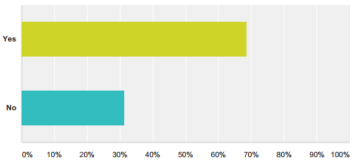
Answered: 17 Skipped: 0




| Answer Choices | Responses | |
|---|---|---|
| Windows (older) | 5.88% | 1 |
| Windows 7 | 82.35% | 14 |
| Windows 8 | 29.41% | 5 |
| Apply Mac (older) | 0.00% | 0 |
| Apple Mac (OS X) | 35.29% | 6 |
| Linux | 29.41% | 5 |
| Other (please specify) | 0.00% | 0 |
| Total Respondents: 17 | | |

**Q4 Are Employees permitted to use their own devices?**

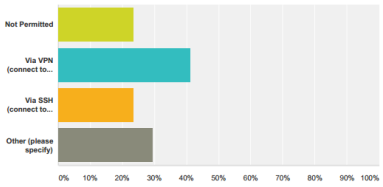
Answered: 16 Skipped: 1




| Answer Choices | Responses | |
|---|---|---|
| Yes | 68.75% | 11 |
| No | 31.25% | 5 |
| Total | | 16 |

**Q5 How may Employees access the work network from home?**

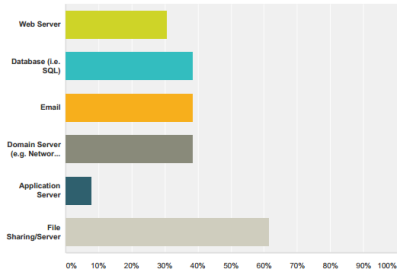
Answered: 17 Skipped: 0




| Answer Choices | Responses | |
|---|---|---|
| Not Permitted | 23.53% | 4 |
| Via VPN (connect to network) | 41.18% | 7 |
| Via SSH (connect to server) | 23.53% | 4 |
| Other (please specify) | 29.41% | 5 |
| Total Respondents: 17 | | |

**Q6 If any, what local services are provided?**

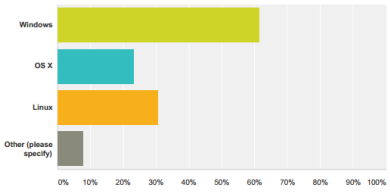
Answered: 13 Skipped: 4




| Answer Choices | Responses | |
|---|---|---|
| Web Server | 30.77% | 4 |
| Database (i.e. SQL) | 38.46% | 5 |
| Email | 38.46% | 5 |
| Domain Server (e.g. Network Security Management) | 38.46% | 5 |
| Application Server | 7.69% | 1 |
| File Sharing/Server | 61.54% | 8 |
| Total Respondents: 13 | | |

**Q7 Which Operating Systems are used to provide local services?**

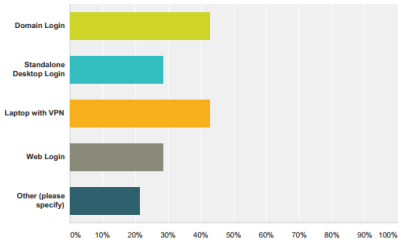
Answered: 13 Skipped: 4




| Answer Choices | Responses | |
|---|---|---|
| Windows | 61.54% | 8 |
| OS X | 23.08% | 3 |
| Linux | 30.77% | 4 |
| Other (please specify) | 7.69% | 1 |
| Total Respondents: 13 | | |

## Q8 How do employees access the local services provided by the company?

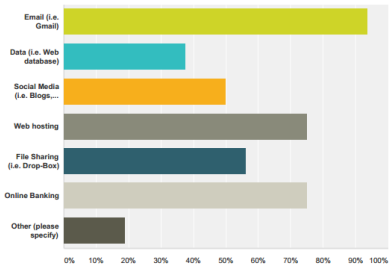
Answered: 14 Skipped: 3




| Answer Choices | Responses | |
|---|---|---|
| Domain Login | 42.86% | 6 |
| Standalone Desktop Login | 28.57% | 4 |
| Laptop with VPN | 42.86% | 6 |
| Web Login | 28.57% | 4 |
| Other (please specify) | 21.43% | 3 |
| Total Respondents: 14 | | |

## Q9 If any, which third-party remote services may be used by employees?

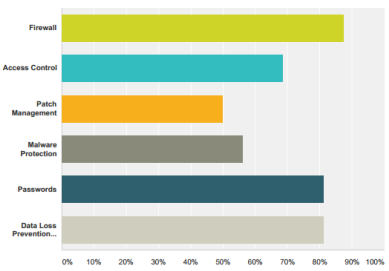
Answered: 16 Skipped: 1




| Answer Choices | Responses | |
|---|---|---|
| Email (i.e. Gmail) | 93.75% | 15 |
| Data (i.e. Web database) | 37.50% | 6 |
| Social Media (i.e. Blogs, Facebook, etc.) | 50.00% | 8 |
| Web hosting | 75.00% | 12 |
| File Sharing (i.e. Drop-Box) | 56.25% | 9 |
| Online Banking | 75.00% | 12 |
| Other (please specify) | 18.75% | 3 |
| Total Respondents: 16 | | |

## Q10 Is there a current security policy in place for any of the following?

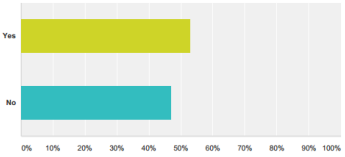
Answered: 16 Skipped: 1




| Answer Choices | Responses | |
|---|---|---|
| Firewall | 87.50% | 14 |
| Access Control | 68.75% | 11 |
| Patch Management | 50.00% | 8 |
| Malware Protection | 56.25% | 9 |
| Passwords | 81.25% | 13 |
| Data Loss Prevention (i.e. printer restrictions, USB-device restrictions, data back-ups) | 81.25% | 13 |
| Total Respondents: 16 | | |

## Q11 Are you aware of the Cyber Essentials scheme?

Answered: 17 Skipped: 0




| Answer Choices | Responses | |
|---|---|---|
| Yes | 52.94% | 9 |
| No | 47.06% | 8 |
| Total | | 17 |