Common Vulnerability Scoring System v3.0

Examples

Version 1.5 September 2017

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0.0 to 10.0, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides a collection of examples of vulnerabilities scored using CVSS v3.0.

Contents

Revision History

Document Revision	Revision Date	Description of Change
1.1	June 2015	First public release.
1.2	January 2016	Changed phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937) to add a discussion of the impact of the HttpOnly flag.
1.3	July 2016	Added Google Chrome PDFium JPEG 2000 Remote Code Execution Vulnerability (CVE-2016-1645). Added SAMR/LSAD Privilege Escalation via Protocol Downgrade Vulnerability ("Badlock") (CVE-2016-0128 and CVE-2016-2118).
1.4	August 2017	Replaced link to XML schema with a link to new web page referencing both JSON and XML schemas.
1.5	September 2017	Updated the email address to use for feedback.

Resources & Links

Below, are useful references to additional CVSS v3.0 documents.

Resource	Location
Specification Document	Includes metric descriptions, formulas, and vector string. Available at http://www.first.org/cvss/specification-document
User guide	Includes further discussion of CVSS v3.0, a scoring rubric, and a glossary. Available at http://www.first.org/cvss/user-guide
Example document	Includes examples of CVSS v3.0 scoring in. practice. Available at https://www.first.org/cvss/examples
CVSS v3.0 logo	Low and hi-res images available at http://www.first.org/cvss/identity
CVSS v3.0 calculator	Reference implementation of the CVSS v3.0 equations, available at https://www.first.org/cvss/calculator/3.0

JSON and XML schemas	JSON and XML schema definitions available at, https://www.first.org/cvss/data-representations

Notes from the CVSS SIG regarding sample vulnerabilities

The following vulnerabilities were scored utilizing public information beyond the CVE summary (may include original bug identification postings, 3rd party exploit analysis, or technical documentation for the vulnerable software). This was done in an attempt to produce richer context for each vulnerability, and more meaningful discussion for our metric decisions. We understand that those running massive vulnerability databases cannot afford to spend the time necessary to research all vulnerabilities to this degree.

Please contact us at cvss@first.org if:

- You have additional, verifiable, information that will change the outcome of one of the scored vulnerabilities.
- You have CVEs for additional vulnerability types that you would like to see added.

phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)

Vulnerability

Reflected cross-site scripting (XSS) vulnerabilities are present on the tbl_gis_visualization.php page in phpMyAdmin 3.5.x, before version 3.5.8. These allow remote attackers to inject arbitrary JavaScript or HTML via the (1) visualizationSettings[width] or (2) visualizationSettings[height] parameters.

Attack

A successful exploit requires an attacker to perform reconnaissance of the system running the vulnerable phpMyAdmin software to determine a valid database name and obtain a valid session token. The attacker constructs a URL to the web server running the vulnerable phpMyAdmin software that contains this database name and token. One of the two injectable parameters is added to the URL with its value set to the malicious code that the attacker wishes a victim to run. The attacker distributes this URL and entices a victim to click on it, e.g. by sending the URL in emails or by adding it to a legitimate web site. If a victim clicks the URL, the malicious code will execute in the victim's web browser. The malicious code is only able to access information associated with the web site running the vulnerable phpMyAdmin software due to Same Origin Policy (SOP) restrictions in web browsers. phpMyAdmin, by default, sets the **HttpOnly** flag on its cookies, preventing JavaScript from accessing the contents web browser cookies which limits the overall impact of this attack.

CVSS v2 Base Score: 4.3

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	None
Integrity Impact	Partial
Availability Impact	None

CVSS v3.0 Base Score: 6.1

Metric	Value	Comments
Attack Vector	Network	The vulnerability is in the web application and reasonably requires network interaction with the server.
Attack Complexity	Low	Although an attacker needs to perform some reconnaissance of the target system, a valid session token can be easily obtained and many systems likely use well-known or default database names.

Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	Required	A successful attack requires the victim to visit the vulnerable component, e.g. by clicking a malicious URL.
Scope	Changed	The **vulnerable component** is the web server running the phpMyAdmin software. The **impacted component** is the victim's browser.
Confidentiality Impact	Low	Information maintained in the victim's web browser can be read and sent to the attacker. This is constrained to information associated with the web site running phpMyAdmin, and cookie data is excluded because the HttpOnly flag is enabled by default by phpMyAdmin. If the HttpOnly flag is not set, the Confidentiality Impact will become High if the attacker has access to sufficient cookie data to hijack the victim's session.
Integrity Impact	Low	Information maintained in the victim's web browser can be modified, but only information associated with the web site running phpMyAdmin.
Availability Impact	None	The malicious code can deliberately slow the victim's system, but the effect is usually minor and the victim can easily close the browser tab to terminate it.

MySQL Stored SQL Injection (CVE-2013-0375)

Vulnerability

A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that MySQL replication functionality would run with high privileges. A successful attack could allow any data in a remote MySQL database to be read or modified.

Attack

An attacker requires an account on the target MySQL database with the privilege to modify user-supplied identifiers, such as table names. The account must be on a database which is being replicated to one or more other MySQL databases. An attack consists of logging in using the account and modifying an identifier to a new value that contains a quote character and a fragment of malicious SQL. This SQL will later be executed as a highly privileged user on the remote system(s). The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.

CVSS v2 Base Score: 5.5

Metric	Value
Access Vector	Network
Access Complexity	Low

Authentication	Single
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS v3.0 Base Score: 6.4

Metric	Value	Comments
Attack Vector	Network	The attacker connects to the exploitable MySQL database over a network.
Attack Complexity	Low	Replication must be enabled on the target database. Although disabled by default, it is common for it to be enabled so we assume this worst case.
Privileges Required	Low	The attack requires an account with the ability to change user-supplied identifiers, such as table names. Basic users do not get this privilege by default, but it is not considered a sufficiently trusted privilege to warrant this metric being **High**.
User Interaction	None	
Scope	Changed	The **vulnerable component** is the MySQL server database and the **impacted component** is a remote MySQL server database (or databases).
Confidentiality Impact	Low	The injected SQL runs with high privilege and can access information the attacker should not have access to. Although this runs on a remote database (or databases), it may be possible to exfiltrate the information as part of the SQL statement. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Integrity Impact	Low	The injected SQL runs with high privilege and can modify information the attacker should not have access to. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Availability Impact	None	Although injected code is run with high privilege, the nature of this attack prevents arbitrary SQL statements being run that could affect the availability of MySQL databases.

SSLv3 POODLE Vulnerability (CVE-2014-3566)

Vulnerability

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for **man in the middle** attackers to obtain plaintext data via a padding-oracle attack, aka the "POODLE" issue.

Attack

A typical attack scenario is that a victim has visited a web server and her web browser now contains a cookie that an attacker wishes to steal. For a successful attack, the attacker must be able to modify network traffic between the victim and this web server, and both victim and system must be willing to use SSL 3.0 for encryption.

A typical attack starts by the attacker tricking the victim into visiting a web site containing malicious code that then runs on the victim's web browser. Same Origin Policy (SOP) restrictions in web browsers prevent this code from directly accessing the cookie the attacker is trying to steal, but HTTP requests that the code sends to the web server automatically have the cookie added, and this behavior is used in the attack.

The malicious code sends an HTTP request that guesses the value of the first byte of the cookie, and positions this byte in a specific location. The attacker modifies the encrypted HTTP request such that this byte is used as a padding value. If the server accepts the modified request, the value guessed was correct; if not, the code guesses a different value in a new request. This process is repeated until the entire cookie is disclosed.

CVSS v2 Base Score: 4.3

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	None
Availability Impact	None

CVSS v3.0 Base Score: 3.1

Metric	Value	Comments
Attack Vector	Network	The attack is conducted over a network. Note that the attack can take place at *any* point between the victim and web server over which the network traffic is routed. The value is therefore Network rather than Adjacent Network; the latter is only used for attacks where the attacker *must* be on the same physical network (or equivalent).
Attack Complexity	High	This is a *man in the middle* attack, and therefore complex for the attacker to perform.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	Required	The victim must be tricked into running malicious code on her web browser.
Scope	Unchanged	The **vulnerable component** is the web server because it insecurely responds to padding errors in a way that can be used to brute force encrypted data. The **impacted component** is also the web server because the cookie information disclosed is part of its authorization authority.
Confidentiality Impact	Low	The attack discloses cookie information that the attacker should not have access to.
Integrity Impact	None	
Availability Impact	None	

VMware Guest to Host Escape Vulnerability (CVE-2012-1516)

Vulnerability

Due to a flaw in the handler function for RPC commands, it is possible to manipulate data pointers within the Virtual Machine Executable (VMX) process. This vulnerability may allow a user in a Guest Virtual Machine to crash the VMX process resulting in a Denial of Service (DoS) on the host or potentially execute code on the host.

Attack

A successful exploit requires an attacker to have access to a Guest Virtual Machine (VM). The Guest VM needs to be configured to have 4GB or more of memory. The attacker would then have to construct a specially crafted remote RPC call to exploit the VMX process.

The VMX process runs in the VMkernel that is responsible for handling I/O to devices that are not critical to performance. It is also responsible for communicating with user interfaces, snapshot managers, and remote console. Each virtual machine has its own VMX process which interacts with the host processes via the VMkernel.

The attacker can exploit the vulnerability to crash the VMX process resulting in a DoS of the host or potentially execute code on the host OS.

CVSS v2 Base Score: 9.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 9.9

Metric	Value	Comments
Attack Vector	Network	VMX process is bound to the network stack and the attacker can send RPC commands remotely.
Attack Complexity	Low	The only required condition for this attack is for virtual machines to have 4GB of memory. Virtual machines that have less than 4GB of memory are not affected.
Privileges Required	Low	The attacker must have access to the Guest VM. This is easy in a tenant environment.
User Interaction	None	The attacker requires no user interaction to successfully exploit the vulnerability. RPC commands can be sent anytime.
Scope	Changed	The **vulnerable component** is a VMX process that can only be accessed from the Guest VM. The **impacted component** is the host OS which has separate authorization authority from the Guest VM.
Confidentiality Impact	High	Full compromise of host OS via remote code execution.
Integrity Impact	High	Full compromise of host OS via remote code execution.
Availability Impact	High	Full compromise of host OS via remote code execution.

Apache Tomcat XML Parser Vulnerability (CVE-2009-0783)

Vulnerability

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 permits web applications to replace an XML parser used for other web applications, which allows local users to read or modify the (1) web.xml, (2) context.xml, or (3) tld files of arbitrary web applications via a crafted application that is loaded earlier than the target application.

Attack

This Tomcat vulnerability allows a web-apps to reference a XML parser instead of using the default Apache XML parser. The attacker must remove all existing web-apps including those in server/webapps, then install a web-app with an XML parser is stored in WEB-INF/lib. This will cause Tomcat to use the new XML parser to process all web.xml, context.xml and tld files of other webapps. If that non-standard XML parser is replaced with a malicious one, the content of the victim web app XML can be disclosed, the resulting JSP could be corrupted (if it compiled at all) or possibly even weaponized for further attacks.

There are 2 different ways this attack may manifest. First a local privileged user could simply replace the non-Apache XML parser with a malicious variant. The second is that an attacker may use social engineering and user interaction to inject the malicious XML parser into the system. We will score for the former.

CVSS v2 Base Score: 4.6

Metric	Value
Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS v3.0 Base Score: 4.2

Metric	Value	Comments
Attack Vector	Local	Local user access is required to read/modify Tomcat configuration files.
Attack Complexity	Low	No special knowledge is necessary to impact XML parser integrity.
Privileges Required	High	The user requires high privileges to be able to modify Tomcat configuration files.
User Interaction	None	

Scope	Unchanged	Assuming simple webapps that do not maintain separate authorization authority.
Confidentiality Impact	Low	Webapp xml and tld files can be exposed.
Integrity Impact	Low	The integrity of the XML parser is lost, possibly resulting in a corrupt JSP.
Availability Impact	Low	The reasonable outcome behind modifying the XML parser is to make certain web applications unavailable.

Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)

Vulnerability

Cisco IOS 12.2 through 12.4 and 15.0 through 15.2 and IOS XE 2.1.x through 2.6.x and 3.1.xS before 3.1.2S, 3.2.xS through 3.4.xS before 3.4.2S, 3.5.xS before 3.5.1S, and 3.1.xSG and 3.2.xSG before 3.2.2SG, when AAA authorization is enabled, allow remote authenticated users to bypass intended access restrictions and execute commands via a (1) HTTP or (2) HTTPS session, aka Bug ID CSCtr91106.

Attack

This vulnerability is post authentication on the administrative interface of the Cisco device. Therefore to attack a typical installation, the attacker would need access to the trusted / internal side of the IOS. This significantly limits the number of potential attackers. However, access to that network is beyond the scope of our score. The vulnerability is due to an error in the (user profile) HTTP/HTTPS AAA authorization implementation, allowing an authenticated user the ability to execute any arbitrary Cisco IOS Software commands configured for the privilege level of the user.

http://tools.cisco.com/security/center/viewAlert.x?alertId=25363

CVSS v2 Base Score: 8.5

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	Single
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 8.8

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	Specialized conditions or advanced knowledge is not required. Access to the protected network is beyond the scope of Attack Complexity.
Privileges Required	Low	Administrative privileges are not required.
User Interaction	None	
Scope	Unchanged	The vulnerability allows authorization bypass, but impact is contained to the original scope of vulnerable component.
Confidentiality Impact	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on Confidentiality of the device.
Integrity Impact	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on Integrity of the device.
Availability Impact	High	Successful exploitation could result in a complete compromise of the targeted device which results in a complete (High) impact on the Availability of the device.

Apple iWork Denial of Service Vulnerability (CVE-2015-1098)

Vulnerability

iWork in Apple iOS before 8.3 and Apple OS X before 10.10.3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted iWork file.

Attack

A remote user can create a specially crafted iWork file that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code. The attacker must deliver and then convince the local user to open the malicious iWork file.

CVSS v2 Base Score: 6.8

Metric	Value
Access Vector	Network
Access Complexity	Medium

Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS v3.0 Base Score: 7.8

Metric	Value	Comments
Attack Vector	Local	The vulnerability is in the local parser.
Attack Complexity	Low	Specialized conditions or advanced knowledge is not required.
Privileges Required	None	
User Interaction	Required	The victim needs to open the malicious iWork file.
Scope	Unchanged	
Confidentiality Impact	High	Arbitrary Code Execution
Integrity Impact	High	Arbitrary Code Execution
Availability Impact	High	Arbitrary Code Execution

OpenSSL Heartbleed Vulnerability (CVE-2014-0160)

Vulnerability

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.

Attack

A successful attack requires only sending a specially crafted message to a web server running OpenSSL. The attacker constructs a malformed "heartbeat request" with a large field length and small payload size. The vulnerable server does not validate that the length of the payload against the provided field length and will return up to 64 kB of server memory to the attacker. It is likely that this memory was previously utilized by OpenSSL. Data returned may contain sensitive information such as encryption keys or user names and passwords that could be used by the attacker to launch further attacks

CVSS v2 Base Score: 5.0

Metric	Value

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	None
Availability Impact	None

CVSS v3.0 Base Score: 7.5

Metric	Value	Comments
Attack Vector	Network	The vulnerability is in a network service that uses OpenSSL.
Attack Complexity	Low	An attacker needs to only find a listening network service to mount an attack.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	None	No user access is required for an attacker to launch a successful attack.
Scope	Unchanged	The **vulnerable component** is OpenSSL which is integrated with the network service, therefore no change in scope occurs during the attack.
Confidentiality Impact	High	Access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact to the affected scope (e.g. the attacker can read the administrator's password, or private keys in memory are disclosed to the attacker).
Integrity Impact	None	No information can be modified by the attacker.
Availability Impact	None	The attacker cannot affect availability through this attack.

GNU Bourne-Again Shell (Bash) ‘Shellshock’ Vulnerability (CVE-2014-6271)

Vulnerability

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."

Attack

A successful attack can be launched by an attacker directly against the vulnerable GNU Bash shell, or in certain cases, by an unauthenticated, remote attacker through services either written in GNU Bash or services spawning GNU Bash shells. In the case of an attack against the Apache HTTP Server running dynamic content CGI modules, an attacker can submit a request while providing specially crafted commands as environment variables. These commands will be interpreted by the handler program, the GNU Bash shell, with the privilege of the running HTTPD process. As such, environment variables passed by the attacker could allow installation of software, account enumeration, denial of service, etc. Attacks against other services that have a relationship with the GNU Bash shell are similarly possible.

CVSS v2 Base Score: 10.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 9.8

Metric	Value	Comments
Attack Vector	Network	Considering the worst case scenario: (web server attack vector).
Attack Complexity	Low	An attacker needs to only gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly.
Privileges Required	None	Some attack vectors do not require any privileges (e.g. CGI in web server).
User Interaction	None	No user interaction is required for an attacker to launch a successful attack.
Scope	Unchanged	The **vulnerable component** is the GNU Bash shell which is used as an interpreter for various services or can be accessed directly, therefore no change in scope occurs during the attack.

Confidentiality Impact	High	Allows an attacker to take complete control of the affected system.
Integrity Impact	High	Allows an attacker to take complete control of the affected system.
Availability Impact	High	Allows an attacker to take complete control of the affected system.

DNS Kaminsky Bug (CVE-2008-1447)

Vulnerability

The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."

Attack

A successful exploit requires an attacker to identify a recursive nameserver running an implementation of DNS that does not supply sufficient randomization of DNS query/transaction IDs combined with sufficient randomization of source ports. The attacker then must configure a nameserver to be authoritative for a target domain. The attacker then queries the victim recursive nameserver for a name within the target domain. Immediately after this request is sent the attacker sends a flood of crafted responses to the victim recursive nameserver attempting to properly guess the query/transaction ID and source port combination. If the crafted response successfully matches and arrives prior to a legitimate answer from the actual authoritative source, the victim recursive nameserver will accept the crafted response and any information within it. This response data will then be stored in the recursive server cache and remain there based on the TTL parameters specified by the attacker in the response. All queries then sent to the victim recursive nameserver will be answered by the poisoned cache and redirect traffic to the attacker's malicious nameserver and thus direct traffic where ever the attacker wishes.

CVSS v2 Base Score: 5.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	None
Integrity Impact	Partial
Availability Impact	None

CVSS v3.0 Base Score: 6.8

Metric	Value	Comments
Attack Vector	Network	The attacker is sending the packets over the network.
Attack Complexity	High	The attacker must configure an authoritative source with a public IP to be routed to by the recursive server. The attacker must also beat a race condition to successfully exploit (regardless of how quick that race condition may occur).
Privileges Required	None	
User Interaction	None	
Scope	Changed	The vulnerable component is the DNS server. The impacted component is the victim system who is unknowingly re-directed to unintended network locations based on the malicious DNS answers.
Confidentiality Impact	None	Any confidentiality is secondary.
Integrity Impact	High	The victim user has trusted a poisoned cache and is being directed to any destination the attacker wishes.
Availability Impact	None	Any availability impact is secondary.

*Scored CIA to both vulnerable component and impacted component, however impacts are the same.

Sophos Login Screen Bypass Vulnerability (CVE-2014-2005)

Vulnerability

Sophos Disk Encryption (SDE) 5.x in Sophos Enterprise Console (SEC) 5.x before 5.2.2 does not enforce intended authentication requirements for a resume action from sleep mode, which allows physically proximate attackers to obtain desktop access by leveraging the absence of a login screen.

Attack

When Microsoft Windows systems resume (“wake up”) from sleep or hibernation, the default action is to require the user to re-authenticate. When SDE is installed, this functionality becomes disabled, allowing an attacker who has physical access to the system access without credentials by triggering a resume action.

CVSS v2 Base Score: 6.9

Metric	Value
Access Vector	Local
Access Complexity	Medium
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 6.8

Metric	Value	Comments
Attack Vector	Physical	Requires physical access to the device.
Attack Complexity	Low	
Privileges Required	None	No privileges are required.
User Interaction	None	
Scope	Unchanged	
Confidentiality Impact	High	The attacker has full access to the system.
Integrity Impact	High	The attacker has full access to the system.
Availability Impact	High	The attacker has full access to the system. Regarding availability impact vs. required control of the device. We are measuring the capabilities granted to the attacker from the vulnerability.

Joomla Directory Traversal Vulnerability (CVE-2010-0467)

Vulnerability

Directory traversal vulnerability in the ccNewsletter (com_ccnewsletter) component 1.0.5 for Joomla allows remote attackers to read arbitrary files via a .. (dot dot) in the controller parameter in a ccnewsletter action to index.php.

Attack

A malicious HTTP request that contains the vulnerable component ‘com_ccnewsletter’, and proper series of ‘../’ entries allows an attacker the ability to change from the directory where the webserver is installed to any directory on the file system of the host OS. Depending on the privileges of the web application server, an attacker would be able to view the contents of any file in the directory searched. Scope is changed due to the ability of the vulnerable component to access the affected system outside of the controlling authoritative component.

CVSS v2 Base Score: 5.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	None
Availability Impact	None

CVSS v3.0 Base Score: 5.8

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	
Privileges Required	None	
User Interaction	None	
Scope	Changed	It is not clear from the publicly available information if Joomla's own authorization authority is enabled or plays a role here. For this vulnerability we are assuming that Joomla has its own separate authorization authority and the attacker is able to break out from it and access files on the file system with privileges of web server which has a separate authorization authority.
Confidentiality Impact	Low	The attacker is able to read files to which web server has access.
Integrity Impact	None	There is no indication that the files can be modified as well.
Availability Impact	None	No availability impact.

Cisco Access Control Bypass Vulnerability (CVE-2012-1342)

Vulnerability

The Cisco Carrier Routing System (CRS-X) running IOS XR Software versions 3.9, 4.0, and 4.1 allows remote attackers to bypass ACL entries via fragmented packets, aka Bug ID CSCtj10975. The vulnerability allows an unauthenticated, remote attacker to bypass device Access Control Entries (ACEs) and send network traffic that should be denied. It only affects devices that have specific ACE structures.

Attack

Exploitation of this vulnerability can be performed with wide-area network access to the target system and requires the ability to send fragmented IPv4 packets to the vulnerable component (router). An attacker can effectively bypass protocol-based access control for non-initial fragments (fragments with a fragment offset not equal to zero), resulting in an integrity impact on the network or devices under the protection of the firewall.

CVSS v2 Base Score: 5.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	None
Integrity Impact	Partial
Availability Impact	None

CVSS v3.0 Base Score: 5.8

Metric	Value	Comments
Attack Vector	Network	The attacker can be multiple hops away from the vulnerable component.
Attack Complexity	Low	The complexity of creating packets that match the criteria (non-first fragments) is low.
Privileges Required	None	A non-privileged user can initiate the packet stream.
User Interaction	None	The attack does not rely on any user interaction.
Scope	Changed	The **vulnerable component** is the CRS itself, while the **impacted component** is the network and devices protected downstream by the CRS.

Confidentiality Impact	None	Impact is scored against the network and devices beyond the firewall (impacted component), and not the CRS (vulnerable component). Any confidentiality loss is a secondary impact.
Integrity Impact	Low	Exploitation results in an integrity impact on the network or devices (impacted component) under the protection of the CRS (vulnerable component).
Availability Impact	None	Impact is scored against the network and devices beyond the firewall (impacted component), and not the CRS (vulnerable component). Any availability is a secondary impact (for example, targeted DoS attack).

Juniper Proxy ARP Denial of Service Vulnerability (CVE-2013-6014)

Vulnerability

If Proxy ARP is enabled on an unnumbered interface, an attacker can poison the ARP cache and create a bogus forwarding table entry for an IP address, effectively creating a denial of service for that subscriber or interface. When Proxy ARP is enabled on an unnumbered interface, the router will answer any ARP message from any IP address which could lead to exploitable information disclosure. This issue can affect any product or platform running Junos OS 10.4, 11.4, 11.4X27, 12.1, 12.1X44, 12.1X45, 12.2, 12.3, or 13.1, supporting unnumbered interfaces.

Attack

Exploitation of this vulnerability requires network adjacency with the target system and the ability to generate arbitrary ARP replies sent to the connected interface. A rogue subscriber can poison the ARP cache and/or create a rogue forwarding table entry for an IP of choice, effectively obscuring that IP address or redirecting IP traffic to the attacker.

The resultant impact can be observed as unauthorized modification of a database on the vulnerable component, or as an impact on confidentiality or availability on attached devices (impacted component). Since the CVSSv3 score for a high confidentiality (or availability) impact on a changed scope is higher than a partial impact on the vulnerable component, CVSSv3 guidance recommends to score for the higher overall impact.

CVSS v2 Base Score: 6.1

Metric	Value
Access Vector	Adjacent Network
Access Complexity	Low

Authentication	None
Confidentiality Impact	None
Integrity Impact	Complete
Availability Impact	None

CVSS v3.0 Base Score: 9.3

Metric	Value	Comments
Attack Vector	Adjacent Network	Exploitation of this vulnerability requires network adjacency with the target system.
Attack Complexity	Low	The complexity of crafting ARP packets to exploit the vulnerability is low.
Privileges Required	None	A non-privileged user can generate the ARP packets.
User Interaction	None	The attack does not rely on any user interaction.
Scope	Changed	The **vulnerable component** is the Junos device itself, while the **impacted component** is any device for which the ARP entry is poisoned.”
Confidentiality Impact	High	The attacker can read any traffic intended for the targeted subscriber(s).
Integrity Impact	None	While modification of the routing table on the vulnerable component would represent an impact on integrity, the Integrity impact on the downstream (impacted) component is None.
Availability Impact	High	Impact on Availability for the downstream (impacted) component results in a complete denial of service for the targeted subscriber(s).

DokuWiki Reflected Cross-site Scripting Attack (CVE-2014-9253)

Vulnerability

DokuWiki contains a reflected cross-site scripting (XSS) vulnerability. This vulnerability allows an attacker with privileges to upload a malicious SWF file to a vulnerable site to perform XSS attacks against victims who follow crafted links to those malicious SWF files. Victims following those crafted links would execute arbitrary script in the victim's browser session within the trust relationship between their browser and the vulnerable server.

Attack

Exploitation of this vulnerability requires an attacker to upload a malicious SWF file to a vulnerable DokuWiki installation, and then send victims a URL to follow which will exploit the XSS attack stored in the SWF file. The resultant impact would be a disclosure of sensitive material or an alteration of page content that should be controlled by the DokuWiki instance (e.g. exposing cookies associated with the wiki, or serving content to the wiki visitor that did not originate at the wiki itself).

Since the vulnerability requires access to upload SWF files, the attacker must have privileges to do this on the wiki itself. And since the vulnerability is exploited at the web server but impacts the victim's browser, scope has changed.

References:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-9253
http://osvdb.org/show/osvdb/115695
http://security.szurek.pl/dokuwiki-20140929a-xss.html

CVSS v2 Base Score: 4.3

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	None
Integrity Impact	Partial
Availability Impact	None

CVSS v3.0 Base Score: 5.4

Metric	Value	Comments
Attack Vector	Network	A victim must access a vulnerable system via the network.
Attack Complexity	Low	
Privileges Required	Low	An attacker must possess "upload" permission to upload a malicious SWF file to the vulnerable wiki.
User Interaction	Required	The user needs to navigate to malicious website.
Scope	Changed	The vulnerability is exploited on the web server, but the impact is to the user's browser.

Confidentiality Impact	Low	Information which should only be disclosed to the vulnerable site, such as cookies, could be provided by the victim’s browser to the attacker
Integrity Impact	Low	Information maintained in the victim's web browser can be modified, but only information associated with the web site running DokuWiki.
Availability Impact	None	

Adobe Acrobat Buffer Overflow Vulnerability (CVE-2009-0658)

Vulnerability

Adobe Acrobat and Reader are vulnerable to a buffer overflow, caused by improper bounds checking when parsing a malformed JBIG2 image stream embedded within a PDF document. By persuading a victim to open a malicious PDF file, a remote attacker could overflow a buffer and execute arbitrary code on the system with the privileges of the victim or cause the application to crash.

Attack

The vulnerability is exploited by convincing a victim to open a malicious document on a system that uses a vulnerable version of Adobe Acrobat or Reader. An attacker must deliver a malicious document to the victim and relies upon the user to open it. If the user is privileged, then the code execution achieved by the attacker could result in High impacts to Confidentiality, Integrity, and Availability.

References:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0658
http://www.adobe.com/support/security/advisories/apsa09-01.html

CVSS v2 Base Score: 9.3

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 7.8

Metric	Value	Comments
Attack Vector	Local	A flaw in the local document software that is triggered by opening a malformed document.
Attack Complexity	Low	
Privileges Required	None	
User Interaction	Required	The victim needs to open the malformed document.
Scope	Unchanged	
Confidentiality Impact	High	Assuming a worst-case impact of the victim having High privileges on the affected system.
Integrity Impact	High	Assuming a worst-case impact of the victim having High privileges on the affected system.
Availability Impact	High	Assuming a worst-case impact of the victim having High privileges on the affected system.

Microsoft Windows Bluetooth Remote Code Execution Vulnerability (CVE-2011-1265)

Vulnerability

The Bluetooth Stack 2.1 in Microsoft Windows Vista SP1 and SP2 and Windows 7 Gold and SP1 does not prevent access to objects in memory that (1) were not properly initialized or (2) have been deleted, which allows remote attackers to execute arbitrary code via crafted Bluetooth packets, aka "Bluetooth Stack Vulnerability."

The vulnerability could allow remote code execution if an attacker sent a series of specially crafted Bluetooth packets to an affected system.

Attack

This vulnerability only affects systems with Bluetooth capability. The attacker first needs to obtain system’s 48-bit Bluetooth address, which is not “discoverable” by default in affected Windows versions. If the system were “discoverable,” it would respond to attacker SDP queries with its Bluetooth address. But in the default state, an attacker must obtain your Bluetooth address another way – either via bruteforcing it or extracting it from Bluetooth traffic captured over-the-air. The attacker would need to be in the same proximity as the target machine in order to send and receive radio transmissions within the Bluetooth radio spectrum. Once it is exploited, the attacker can run arbitrary code. The attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

CVSS v2 Base Score: 8.3

Metric	Value

Access Vector	Adjacent Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 8.8

Metric	Value	Comments
Attack Vector	Adjacent Network	The attacker would need to be in the same proximity as the target machine in order to send and receive radio transmissions within the Bluetooth radio spectrum.
Attack Complexity	Low	We are assuming that Bluetooth is enabled on the OS. The attacker can obtain system's 48-bit Bluetooth address in one of three ways 1) from the beacon messages if the device is "discoverable" 2) via bruteforcing it 3) extracting it from Bluetooth traffic captured over-the-air. At least one of these attack vectors is considered as Low Attack Complexity based on the criteria listed in the specification.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	None	No user interaction is required for this attack.
Scope	Unchanged	The vulnerable component and impacted component are the same, which is operating system.
Confidentiality Impact	High	The attacker can view, change, or delete data; or create new accounts with full user rights.
Integrity Impact	High	The attacker can view, change, or delete data; or create new accounts with full user rights.
Availability Impact	High	The attacker can view, change, or delete data; or create new accounts with full user rights.

Apple iOS Security Control Bypass Vulnerability (CVE-2014-2019)

Vulnerability

The iCloud subsystem in Apple iOS before 7.1 allows physically proximate attackers to bypass an intended password requirement, and turn off the Find My iPhone service or complete a Delete Account action and then associate this service with a different Apple ID account, by entering an arbitrary iCloud Account Password value and a blank iCloud Account Description value.

Attack

Find My iPhone helps you locate and protect your iPhone, iPad, iPod touch, or Mac if it's ever lost or stolen. With Find My iPhone set up on your device, you can do the following:

- Locate your device on a map
- Play a sound on your device to help you find it
- Use Lost Mode to lock and track your device
- Remotely erase all of your personal information from the device

Find My iPhone includes a feature called Activation Lock that is designed to prevent anyone else from using your iPhone, iPad, or iPod touch if it's ever lost or stolen. Activation Lock is enabled automatically when you turn on Find My iPhone on a device using iOS 7 or later. Find My iPhone Activation Lock, your Apple ID and password will be required before anyone can:

- Turn off Find My iPhone on your device
- Erase your device
- Reactivate and use your device

This vulnerability allows the attacker to bypass the Activation Lock when attempting to turn off Find My iPhone. The attacker can turn off Find My iPhone feature, delete the current iCloud account and associate the device with new iCloud Account with out any Apple ID and password of current user.

CVSS v2 Base Score: 4.9

Metric	Value
Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality Impact	None
Integrity Impact	Complete
Availability Impact	None

CVSS v3.0 Base Score: 4.6

Metric	Value	Comments

Attack Vector	Physical	The attacker requires physical access to the device.
Attack Complexity	Low	The attack steps are simple.
Privileges Required	None	We will consider the worse case scenario and assume that the device is not protected with a PIN.
User Interaction	None	No user interaction is required for this attack.
Scope	Unchanged	The **vulnerable** and **impacted components** are the same.
Confidentiality Impact	None	Any confidentiality impact is a secondary impact.
Integrity Impact	High	High due to importance (security) of this feature.
Availability Impact	None	Any availability impact is a secondary.

SearchBlox Cross-Site Request Forgery Vulnerability (CVE-2015-0970)

Vulnerability

SearchBlox is an enterprise search and data analytics service utilizing Apache Lucene and Elasticsearch.

A cross-site request forgery (CSRF) vulnerability in SearchBlox Server before version 8.2 allows remote attackers to perform actions with the permissions of a victim user, provided the victim user has an active session and is induced to trigger the malicious request.

Attack

A specially-crafted URL to the SearchBlox Server containing the appropriate parameter values of an action the attacker wants to perform may be sent to a victim user. This URL may be sent to the victim as part of an HTML document, an email, or via some other method. If the user interacts with the URL while the user has an active session on the SearchBlox Server, the URL will send a request to the server to perform some action with the victim user's credentials. Since SearchBlox Server prior to version 8.2 has no request validation mechanism, the request will be completed if the victim user's permissions allow such an action. Possible actions include creating or deleting a user account, or uploading new SearchBlox configuration settings.

CVSS v2 Base Score: 6.8

Metric	Value
Access Vector	Network
Access Complexity	Medium

Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS v3.0 Base Score: 8.8

Metric	Value	Comments
Attack Vector	Network	A victim must access a vulnerable system via the network.
Attack Complexity	Low	A phishing email does not absolutely require victim reconnaissance.
Privileges Required	None	The attacker does not need any permissions to perform this attack, the attacker lets the victim perform the action on the attacker's behalf.
User Interaction	Required	The victim must click a specially crafted link provided by the attacker.
Scope	Unchanged	The **vulnerable component** is SearchBlox. The **impacted component** is also SearchBlox as the actions only affect the SearchBlox configuration.
Confidentiality Impact	High	The attacker can obtain permissions to view all confidential data contained in SearchBlox.
Integrity Impact	High	User accounts can be modified at will as well as SearchBlox configuration.
Availability Impact	High	SearchBlox configuration may be modified such as to disable services.

SSL/TLS MITM Vulnerability (CVE-2014-0224)

Vulnerability

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server. The attack can only be performed between a vulnerable client *and* server. This is also known as the "CCS Injection" vulnerability, named after the vulnerable ChangeCipherSpec messages.

Attack

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec message during the SSL/TLS handshake. A ChangeCipherSpec message tells the client/server to switch from unencrypted to encrypted communication. If a ChangeCipherSpec message is sent by the attacker after the connection is initiated but before the master secret has been generated, then OpenSSL will generate the keys for the handshake with an empty master secret. This zero-length master key allows an attacker to crack the encryption and consequently obtain sensitive information and/or modify SSL/TLS traffic. Note that an attacker requires a man-in-the-middle position with the client user in order to exploit this attack.

CVSS v2 Base Score: 6.8

Metric	Value
Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS v3.0 Base Score: 7.4

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	High	The attacker must be able to monitor and alter victims' network traffic. Measurable effort is typically required to intercept network traffic in this way, making attack complexity "High".
Privileges Required	None	
User Interaction	None	The attacker does not require the user to perform any actions.
Scope	Unchanged	The **vulnerable component** is OpenSSL. The **impacted component** is also OpenSSL as only the OpenSSL encrypted channel is impacted.
Confidentiality Impact	High	An attacker is able to decrypt all SSL/TLS traffic between the client and server.
Integrity Impact	High	An attacker is able to modify all SSL/TLS traffic between the client and server.
Availability Impact	None	No impact to the availability of the SSL/TLS session, the victim believes the session works correctly.

Google Chrome Sandbox Bypass vulnerability (CVE-2012-5376)

Vulnerability

The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended sandbox restrictions and write to arbitrary files by leveraging access to a renderer process.

Attack

Google Chrome uses a multi-process architecture in which each browser tab may run a separate renderer process that communicates with other Chrome processes using the IPC. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to write arbitrary files to the operating system.

CVSS v2 Base Score: 10.0

Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS v3.0 Base Score: 9.6

Metric	Value	Comments
Attack Vector	Network	The victim must visit a malicious website that may exist outside the local network
Attack Complexity	Low	The attacker does not need to perform any special reconnaissance for this attack
Privileges Required	None	The attacker does not need any permissions to perform this attack, the attacker lets the victim perform the action on the attacker's behalf.
User Interaction	Required	The victim must click a specially crafted link provided by the attacker.

Scope	Changed	Based on the assumption that the attacker is breaking out of Chrome’s controlled sandboxed environment, the vulnerable component is Google Chrome and the impacted component is the operating system on which Chrome is running.
Confidentiality Impact	High	The worst case scenario is Chrome is running with administrative privileges. The attacker can overwrite system configuration and grant the attacker access to any data on the system.
Integrity Impact	High	The worst case scenario is Chrome is running with administrative privileges. The attacker can overwrite any file, including important system files.
Availability Impact	High	The worst case scenario is Chrome is running with administrative privileges. The attacker can cause a system crash by overwriting particular system files.

Google Chrome PDFium JPEG 2000 Remote Code Execution Vulnerability (CVE-2016-1645)

Vulnerability

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Google Chrome. User interaction is required to exploit this vulnerability in that the victim must visit a malicious page or open a malicious file.

The specific flaw exists within the handling of JPEG 2000 images. A specially crafted JPEG 2000 image embedded inside a PDF can force Google Chrome to write memory past the end of an allocated object. An attacker can leverage this vulnerability to execute arbitrary code under the context of the current process.

Attack

An attacker creates a PDF file embedding a maliciously crafted JPEG 2000 image. This is made available to victims, e.g., via a web page. A victim opens the PDF document using a Google Chrome browser, and the browser displays the PDF using the built-in PDFium PDF viewer. This triggers the exploit and runs the executable code that the attacker placed in the image, taking over the browser.

Metric	Value
Access Vector	Network
Access Complexity	Medium

Authentication	None
Confidentiality Impact	Complete
Integrity Impact	Complete
Availability Impact	Complete

Metric	Value	Comments
Attack Vector	Network	Vulnerabilities where the vulnerable component is a separate program invoked from a browser, e.g., a word processor, and which require user interaction to download or receive malicious content which could also be delivered locally, should be scored as *Local*. For example, a document parsing vulnerability which does not require the network in order to be exploited should be scored as *Local*, regardless of the method used to distribute such a malicious document (e.g., it could be a link to a web site, or via a USB drive). However, for this vulnerability, a PDF file opened in Google Chrome is automatically displayed using the PDFium functionality that is part of the browser. In such cases where the victim could load a malicious PDF file *either* via a network *or* from local media (e.g., a hard disk or USB drive), we score Attack Vector as *Network*, as this gives the higher Base Score. Vulnerabilities in functionality added to a browser, e.g., plugins, extensions and add-ons, are treated as part of the browser when determining Attack Vector. For example, a vulnerability in Adobe Flash is scored with an Attack Vector of *Network* (assuming the victim loads the exploit over a network).
Attack Complexity	Low	Specialized access conditions or extenuating circumstances do not exist.
Privileges Required	None	An attacker requires no privileges to mount an attack.
User Interaction	Required	A successful attack requires a victim to open a malicious PDF file.
Scope	Unchanged	The **vulnerable component** is the victim's Google Chrome web browser. The **impacted component** is also the victim's Google Chrome browser.
Confidentiality Impact	High	The Google Chrome web browser is completely compromised and runs executable code created by the attacker.

Integrity Impact	High	The Google Chrome web browser is completely compromised and runs executable code created by the attacker.
Availability Impact	High	The Google Chrome web browser is completely compromised and runs executable code created by the attacker.

SAMR/LSAD Privilege Escalation via Protocol Downgrade Vulnerability (“Badlock”) (CVE-2016-0128 and CVE-2016-2118)

Vulnerability

The Security Account Manager Remote (SAMR) and Local Security Authority (Domain Policy) (LSAD) protocols allow access to Windows domains and network shares via the Server Message Block (SMB) protocol. SAMR/LSAD allow setting an “auth level” which determines how the server authenticates requests. Specifically, setting an auth level of “CONNECT” does not properly sign and authenticate messages. An attacker with a man-in-the-middle position between a victim user and the remote SMB server can send a crafted request to downgrade the authentication level of the connection to “CONNECT”, allowing the attacker to then impersonate a victim, effectively gaining the privileges of the victim user.

Attack

If an attacker maintains a man-in-the-middle position between a victim and a remote SMB server, the attacker can modify requests from the victim to force the SMB server to downgrade its SAMR/LSAD protocols to use an auth level of CONNECT. The attack allows an attacker to access the communication channel used by the victim, and impersonate the victim in transactions due to a lack of proper authentication of messages. Effectively, the user can escalate privileges to the privilege level of the victim user.

CVE-2016-0128 is the variant for Microsoft Windows and requires the victim user to be a domain administrator attempting an uncommon action, such as a domain join, for the attack to succeed. A particular consequence is that the SAM credentials database may be obtained, allowing further network access.

CVE-2016-2118, meanwhile, is the variant for SAMBA and may affect a more typical user performing more common actions such as file or printer sharing.

CVSS v2 Base Score: 5.8 (CVE-2016-0128) vs 6.8 (CVE-2016-2118)

Metric	CVE-2016-0128 Value	CVE-2016-2118 Value
Access Vector	Network	Network
Access Complexity	Medium	Medium
Authentication	None	None
Confidentiality Impact	Partial	Partial
Integrity Impact	Partial	Partial
Availability Impact	None	Partial

CVSS v3.0 Base Score: 6.8 (CVE-2016-0128) vs 7.5 (CVE-2016-2118)

Metric	CVE-2016-0128 Value	CVE-2016-2118 Value	Comments
Attack Vector	Network	Network	This attack is not limited to a collision domain and may be performed against any user on the network for which a man-in-the-middle scenario may be established.
Attack Complexity	High	High	The attacker requires specialized access conditions or extenuating circumstances in order to create a man-in-the-middle scenario. In many circumstances this would require access to a private internal network.
Privileges Required	None	None	No extra privileges are required to mount an attack.
User Interaction	Required	Required	A successful attack requires the victim user to perform a domain join, user account add, printer share, or similar action. The attacker must wait for an action to occur.
Scope	Unchanged	Unchanged	For CVE-2016-0128, the **vulnerable component** is the Windows subsystem consisting of the Windows Domain Controller and associated SAM database, that authenticates the victim's SMB connections. For CVE-2016-2118, the **vulnerable component** is the SAMBA server, that authenticates the victim's SMB connections. For both vulnerabilities, the **impacted component** is the same as the vulnerable component.
Confidentiality Impact	High	High	An attacker can spoof a user and access the victim user's resources on the vulnerable server. The attacker is assumed to target a highly privileged user. For CVE-2016-0128, a successful attack results in access to all data stored in the SAM. For CVE-2016-2118, although the attacker may not gain access to all data stored in the SAMBA server, it includes data considered to have a direct, serious impact. Confidentiality is therefore High in both cases.
Integrity Impact	High	High	An attacker can spoof a user and modify any of the user's resources on the vulnerable server. The protocol downgrade removes the ability for the server to detect the manipulation. The attacker is assumed to target a highly privileged user. For CVE-2016-0128, a successful attack results in the ability to modify all data stored in the SAM.

			For CVE-2016-2118, although the attacker may not gain the ability to modify all data stored in the SAMBA server, modification of data considered to have a direct, serious impact is possible. Confidentiality is therefore High in both cases.
Availability Impact	None	High	For CVE-2016-0128, an attacker cannot immediately influence the availability of the service, therefore the Availability is None. For CVE-2016-2118, an attacker can immediately read/write files to a file or printer server, potentially degrading service or even shutting it down, so the impact is High.