CVSS v3.0 Preview 2: Metrics / Formula / Examples
FIRST.ORG
December 2014

Contents

“Scope change” examples

Reflective XSS (CVE-2013-1937)

Multiple cross-site scripting (XSS) vulnerabilities in tbl_gis_visualization.php in phpMyAdmin 3.5.x before 3.5.8 might allow remote attackers to inject arbitrary web script or HTML via the (1) visualizationSettings[width] or (2) visualizationSettings[height] parameter.

CVSSv2: 4.3

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

CVSSv3: 6.1

Metric	Value	Comments
Attack Vector	Network	The vulnerability is in the web application.
Attack Complexity	Low	
Privileges Required	None	Reflective XSS. The attacker is unprivileged or unauthenticated.
User Interaction	Required	An attacker relies on user interaction
Scope	Changed	The attacker is attacking the Exploitable Scope of the web server (under the authorization authority of the web server’s OS). And as a result attacker can impact Confidentiality / Integrity on a 3rd party browser (Impact Scope) authorized by the client’s OS

		you have a scope change.
Confidentiality Impact	Low	Low impact based on public information about the vulnerability.
Integrity Impact	Low	Low impact based on public information about the vulnerability.
Availability Impact	None	No known impact on availability of the target service.

Stored XSS (CVE-2014-4722)

Multiple stored cross-site scripting (XSS) vulnerabilities in the OCS Reports Web Interface in OCS Inventory NG allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVSSv2: 3.5

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

CVSSv3: 5.4

Metric	Value	Comments
Attack Vector	Network	Based on CVE description arbitrary web scripts are injected by remote attacker via unspecified vectors.
Attack Complexity	Low	
Privileges Required	Low	Stored XSS. The attacker must authenticate to store the exploit.
User Interaction	Required	An attacker relies on user interaction
Scope	Changed	The attacker is attacking the Exploitable Scope of the web server under the authorization authority of the web server’s OS. And as a result

		attacker can impact Confidentiality / Integrity (Impact Scope) on a 3rd party browser authorized by the web client's OS results in a scope change.
Confidentiality Impact	Low	
Integrity Impact	Low	
Availability Impact	None	

VMWare Vulnerability (CVE-2012-1517)

The VMX process in VMware ESXi 4.1 and ESX 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving function pointers.

CVSSv2: 9.0

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

CVSSv3: 9.9

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	
Privileges Required	Low	Unprivileged authenticated Guest OS user
User Interaction	None	
Scope	Changed	Guest OS and Host OS have separate authorization scopes; Guest OS users are authorized by the Guest OS, and the Host OS trusts the Guest environment to allow RPC commands from the Guest (Exploitable Scope) to impact the environment of the Host (Impact Scope).

Confidentiality Impact	High	The worst case scenario for arbitrary code execution.
Integrity Impact	High	The worst case scenario for arbitrary code execution.
Availability Impact	High	The worst case scenario for arbitrary code execution.

“No scope change” examples

Apache Tomcat Vulnerability (CVE-2009-0783)

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.

CVSSv2: 4.6

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

CVSSv3: 4.4

Metric	Value	Comments
Attack Vector	Local	Local user access to read/modify files.
Attack Complexity	Low	
Privileges Required	Low	Unprivileged web application user
User Interaction	None	
Scope	Unchanged	This is constrained to the Tomcat Exploitable Scope.
Confidentiality Impact	Low	The attacker can read configuration

		files of other web applications.
Integrity Impact	Low	The attacker can modify configuration files of other web applications.
Availability Impact	None	The web server is still running and available. Modification to config file to disable the web app is a secondary impact to the integrity of the configuration file.

Cisco IOS Vulnerability (CVE-2012-0384)

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.

CVSSv2: 8.5

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

CVSSv3: 8.8

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	Low due to non-default configuration.
Privileges Required	Low	
User Interaction	None	
Scope	Unchanged	The vulnerability allows authorization bypass, but impact is contained to the original Exploitable Scope.
Confidentiality Impact	High	Executing commands as “root”
Integrity Impact	High	Executing commands as “root”

Availability Impact	High	Executing commands as “root”

Impact metric examples

OpenSSL Heartbleed (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.

CVSSv2: 5.0

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

CVSSv3: 7.5

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	
Privileges Required	None	
User Interaction	None	
Scope	Unchanged	
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	

Availability Impact	None	

DNS Kaminsky Bug (CVE-2008-1447)

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."

CVSSv2: 6.4

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

CVSSv3: 7.5

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	
Privileges Required	None	
User Interaction	None	
Scope	Unchanged	
Confidentiality Impact	None	Any Confidentiality Impact (access to redirected data) would be secondary to the Integrity impact.
Integrity Impact	High	Affecting integrity of DNS lookup records.
Availability Impact	None	Any availability impact would be secondary to the Integrity Impact

MySQL SQL Injection (CVE-2013-0375)

A vulnerability in earlier versions of 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 the MySQL database to be read or modified.

CVSSv2: 5.5

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

CVSSv3: 8.1

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	Low	
Privileges Required	Low	
User Interaction	None	
Scope	Unchanged	
Confidentiality Impact	High	Under CVSSv2, the Confidentiality, Integrity and Availability metrics are scored relative to the operating system. The highest impact value that can be given to a vulnerability that affects a component, but not the whole operating system, is Partial. CVSSv3 provides more granularities with the introduction of the Scope metric and the fact that vulnerabilities are scored relative to the Impact Scope. In cases where the Confidentiality, Integrity and/or Availability of the Impact Scope are totally compromised (or a lesser impact involves information with a direct, serious impact), CVSSv2 values of Partial are scored as High under CVSSv3.0.
Integrity Impact	High	
Availability Impact	None	None, database is still running.

Attack Vector examples

Local AV File Based Attack (CVE-2013-6801)

Microsoft Word 2003 SP2 and SP3 on Windows XP SP3 allows remote attackers to cause a denial of service (CPU consumption) via a malformed .doc file containing an embedded image, as demonstrated by word2003forkbomb.doc, related to a "fork bomb" issue.

CVSSv2: 7.1

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

CVSSv3: 5.5

Metric	Value	Comments
Attack Vector	Local	A flaw in the local word processing application when processing a malformed document.
Attack Complexity	Low	
Privileges Required	None	
User Interaction	Required	The victim needs to open malformed document.
Scope	Unchanged	
Confidentiality Impact	None	
Integrity Impact	None	
Availability Impact	High	

Physical AV (CVE-2014-2019)

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.

CVSSv2: 4.9

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

CVSSv3: 4.6

Metric	Value	Comments
Attack Vector	Physical	
Attack Complexity	Low	
Privileges Required	None	
User Interaction	None	
Scope	Unchanged	
Confidentiality Impact	None	
Integrity Impact	High	High due to importance (security) of this feature
Availability Impact	None	

Attack Complexity examples

Attack Complexity High (CVE-2014-2200)

Cisco NX-OS 5.0 before 5.0(5) on Nexus 7000 devices, when local authentication and multiple VDCs are enabled, allows remote authenticated users to gain privileges within an unintended VDC via an SSH session to a management interface, aka Bug ID CSCti11629.

CVSSv2: 7.1

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

CVSSv3: 6.6

Metric	Value	Comments
Attack Vector	Network	
Attack Complexity	High	Multiple virtual device contexts (VDC) must exist on the system and local authentication has to be configured.
Privileges Required	High	VDC administrator privilege is required.
User Interaction	None	
Scope	Unchanged	
Confidentiality Impact	High	Allows an attacker to take complete control of the affected device.
Integrity Impact	High	Allows an attacker to take complete control of the affected device.
Availability Impact	High	Allows an attacker to take complete control of the affected device.