27th ANNUAL FIRST CONFERENCE

BERLIN

14 - 19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015

CVSS v3 Hands-on Training

Seth Hanford
Manager, Detection & Response, TIAA-CREF
Chair, CVSS-SIG

CVSS SIG

TIAA CREF Financial Services

27th ANNUAL FIRST CONFERENCE BERLIN
14-19 JUNE 2015

Introduction

Key Goals for v3

Reflect “real life”

- Solve the “Scope” problem (vulnerabilities aren’t all relative to Host OS)
- Address changes in technologies, threats, and vulnerabilities

Better Usability

- Decrease subjectivity / increase objectivity & repeatability
- Increase actionable uses / decrease ineffective measures

Better Reference & Training

- Documentation and examples

Understanding v3 Metrics

Attack Vector

Metric Value	Description
Network (N)	A vulnerability exploitable with network access means the vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer).
Adjacent (A)	A vulnerability exploitable with adjacent network access means the vulnerable component is bound to the network stack, however the attack is limited to the same shared physical (e.g. Bluetooth, IEEE 802.11), or logical (e.g. local IP subnet) network, and cannot be performed across an OSI layer 3 boundary (e.g. a router).
Local (L)	A vulnerability exploitable with local access means that the vulnerable component is not bound to the network stack, and the attacker’s path is via read/write/execute capabilities.
Physical (P)	A vulnerability exploitable with physical access requires the attacker to physically touch or manipulate the vulnerable component.

Attack Complexity

Metric Value	Description
Low (L)	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable success against the vulnerable component.
High (H)	A successful attack depends on conditions beyond the attacker's control. That is, a successful attack cannot be accomplished at will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against the vulnerable component before a successful attack can be expected.

Privileges Required

Metric Value	Description
None (N)	The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.
Low (L)	The attacker is authorized with (i.e. requires) privileges that provide basic user capabilities that could normally affect only settings and files owned by a user. Alternatively, an attacker with Low privileges may have the ability to cause an impact only to non-sensitive resources.
High (H)	The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

User Interaction

Metric Value	Description
None (N)	The vulnerable system can be exploited without interaction from any user.
Required (R)	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited. For example, a successful exploit may only be possible during the installation of an application by a system administrator.

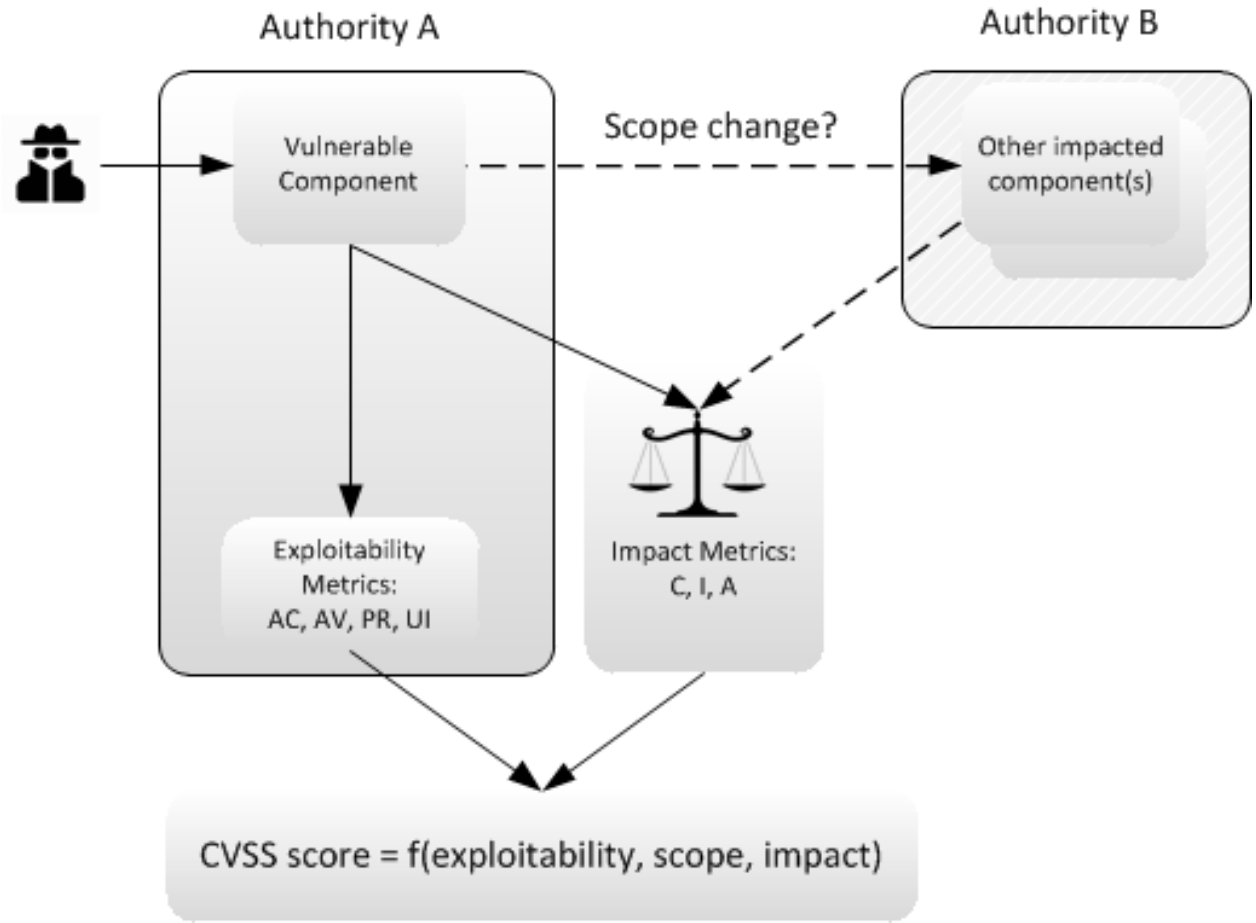
Scope

Metric Value	Description
Unchanged (U)	An exploited vulnerability can only affect resources managed by the same authority. In this case the exploited component and the impacted component are the same.
Changed (C)	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case the exploited component and the impacted component are different.

What is Scope?

- The collection of privileges defined by a computing authority (e.g. an application, an OS, or a sandbox) when granting access to computing resources (e.g. files, CPU, memory, etc.)
- Examples:
  - Operating System
  - Application with users and privileges separate from the OS
  - Hypervisor / Virtual Machine Monitor (VMM)
  - Two distinct systems that share a trust relationship

Scope


Authority A
Authority B
Vulnerable Component
Scope change?
Other impacted component(s)
Exploitability Metrics: AC, AV, PR, UI
Impact Metrics: C, I, A
CVSS score = f(exploitability, scope, impact)

Confidentiality

Metric Value	Description
High (H)	There is total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.
Low (L)	There is some loss of confidentiality. Access to some restricted information is obtained, but the attacker does not have control over what information is obtained, or the amount or kind of loss is constrained. The information disclosure does not cause a direct, serious loss to the impacted component.
None (N)	There is no loss of confidentiality within the impacted component.

Integrity

Metric Value	Description
High (H)	There is a total loss of integrity, or a complete loss of protection. For example, the attacker is able to modify any files protected by the impacted component. Alternatively, only some files can be modified, but malicious modification would present a direct, serious consequence to the impacted component.
Low (L)	Modification of data is possible, but the attacker does not have control over the consequence of a modification, or the amount of modification is constrained. The data modification does not have a direct, serious impact on the impacted component.
None (N)	There is no loss of integrity within the impacted component.

Availability

Metric Value	Description
High (H)	There is total loss of availability, resulting in the attacker being able to fully deny access to resources in the impacted component; this loss is either sustained (while the attacker continues to deliver the attack) or persistent (the condition persists even after the attack has completed). Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious consequence to the impacted component.
Low (L)	There is reduced performance or interruptions in resource availability. The attacker does not have the ability to completely deny service to legitimate users, even through repeated exploitation of the vulnerability. The resources in the impacted component are either partially available all of the time, or fully available only some of the time, but overall there is no direct, serious consequence to the impacted component.
None (N)	There is no impact to availability within the impacted component.

27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015

What's New Since v2.0?

Comparing v2.0 to v3.0

Version 2.0	Version 3.0
Vulnerabilities are scored relative to the overall impact to the host platform.	Vulnerabilities now scored relative to the impact to the impacted component.
No awareness of situations in which a vulnerability in one application impacted other applications on the same system.	A new metric, Scope, now accommodates vulnerabilities where the thing suffering the impact (the impacted component) is different from the thing that is vulnerable (the vulnerable component).
Access Vector may confound attacks that require local system access and physical hardware attacks.	Local and physical values are now separated in the Attack Vector metric.

Comparing v2.0 to v3.0, cont.

Version 2.0	Version 3.0
In some cases, Access Complexity conflated system configuration and user interaction.	This metric has been separated into Attack Complexity (accounting for system complexity), and User Interaction (accounting for user involvement in a successful attack).
In practice, the Authentication metric scores were biased toward two of three possible outcomes, and not effectively capturing the intended aspect of a vulnerability.	A new metric, Privileges Required, replaces Authentication, and now reflects the greatest privileges required by an attacker, rather than the number of times the attacker must authenticate.

Comparing v2.0 to v3.0, cont.

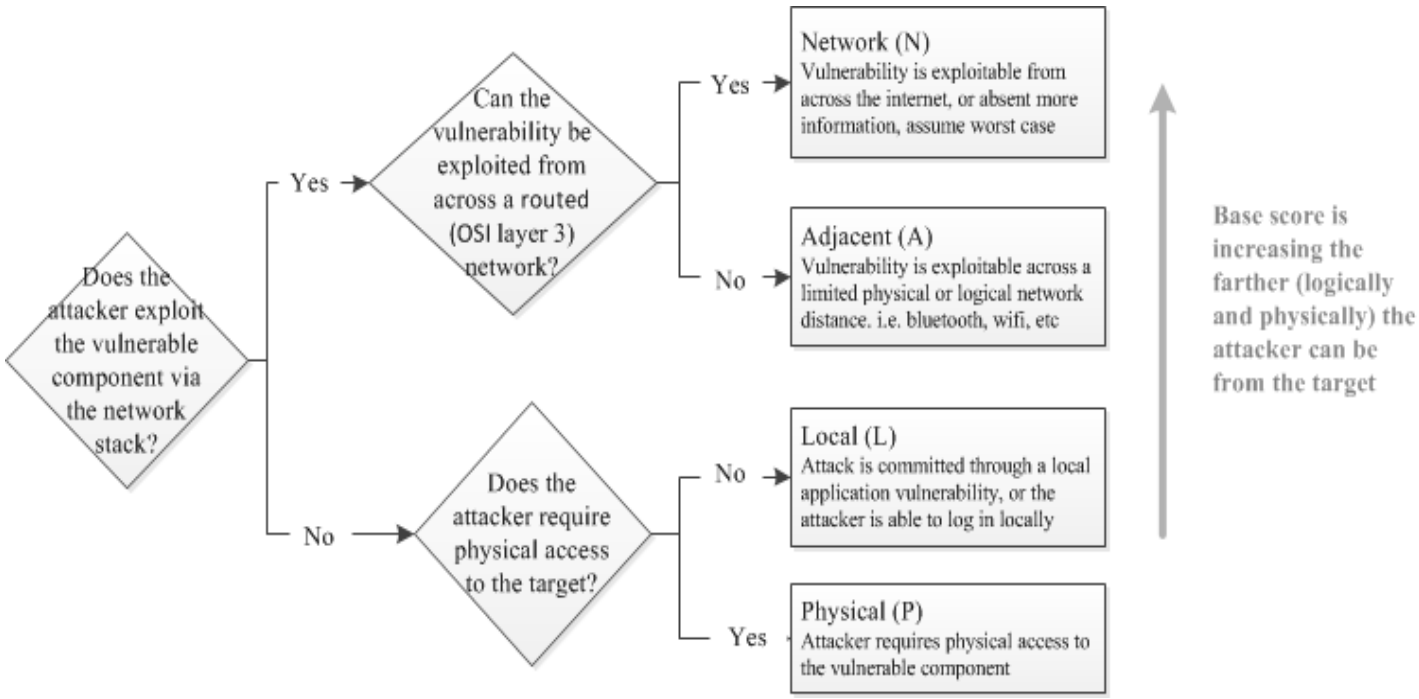
Version 2.0	Version 3.0
Impact metrics reflected percentage of impact caused to a vulnerable application.	Impact metric values now reflect degree of impact, and renamed to “none,” “low,” and “high.”
The Environmental metrics of Target Distribution and Collateral Damage potential were not found to be useful.	Target Distribution and Collateral Damage potential have been replaced with Mitigating Factors.
CVSS v2.0 could not accommodate scoring multiple vulnerabilities used in the same attack.	While not a formal metric, guidance on scoring multiple vulnerabilities is provided with Vulnerability Chaining.
No formal qualitative scoring guidelines were provided.	Numerical ranges have been mapped to a 5-point qualitative rating scale.

Scoring Method

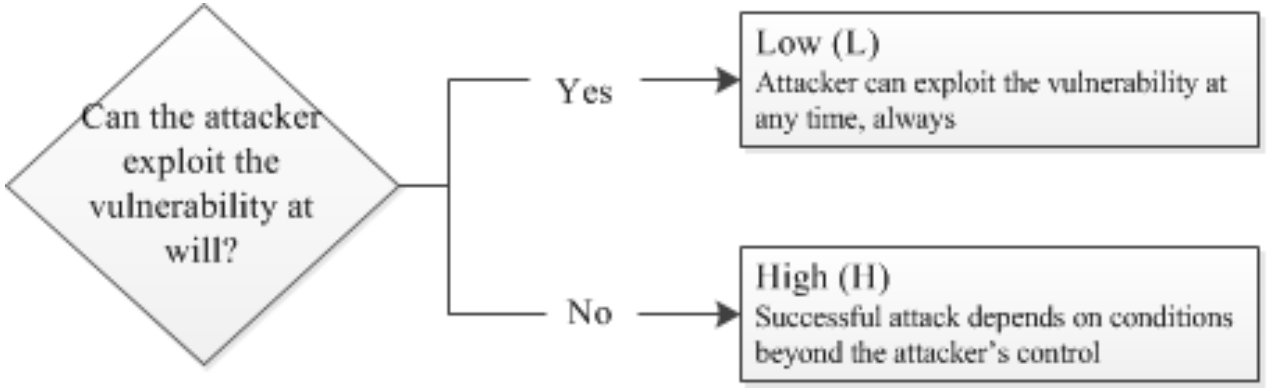
Resources

- Vulnerability Information
- V3 Specification
- V3 Calculator
- V3 Scoring Rubric
- V2 Vulnerability Scores

Attack Vector



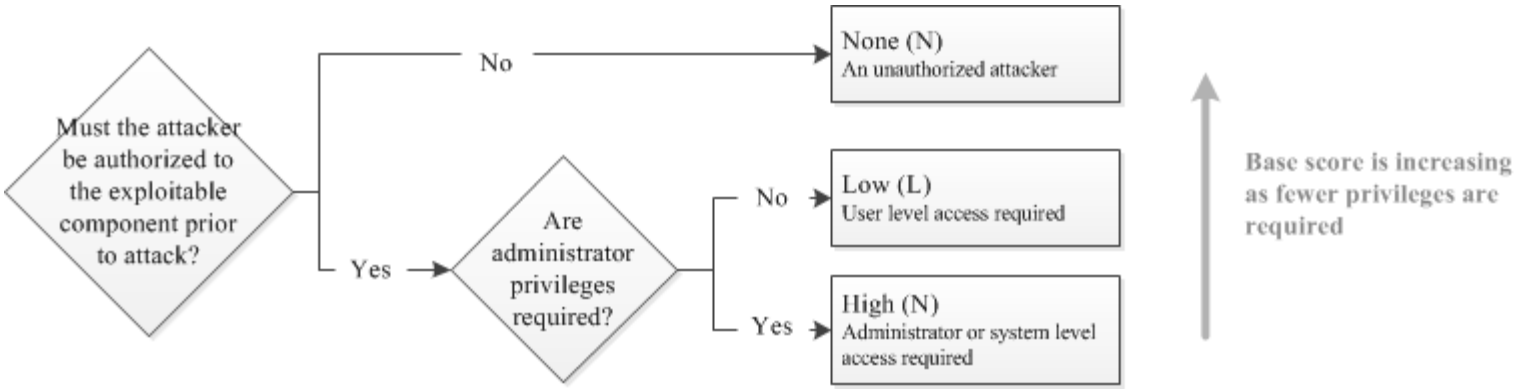
Attack Complexity



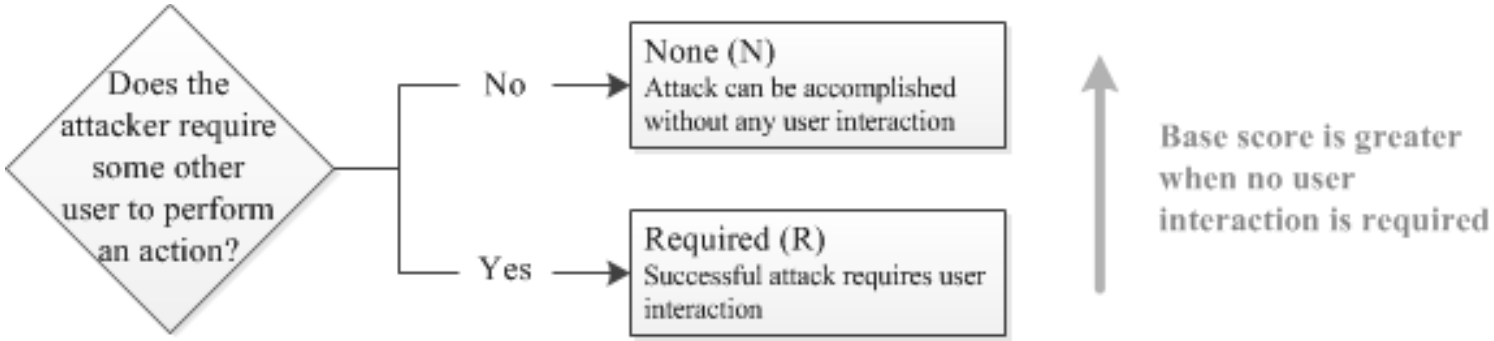
Base score is greater when the attack can be performed at will

Note: this excludes user interaction

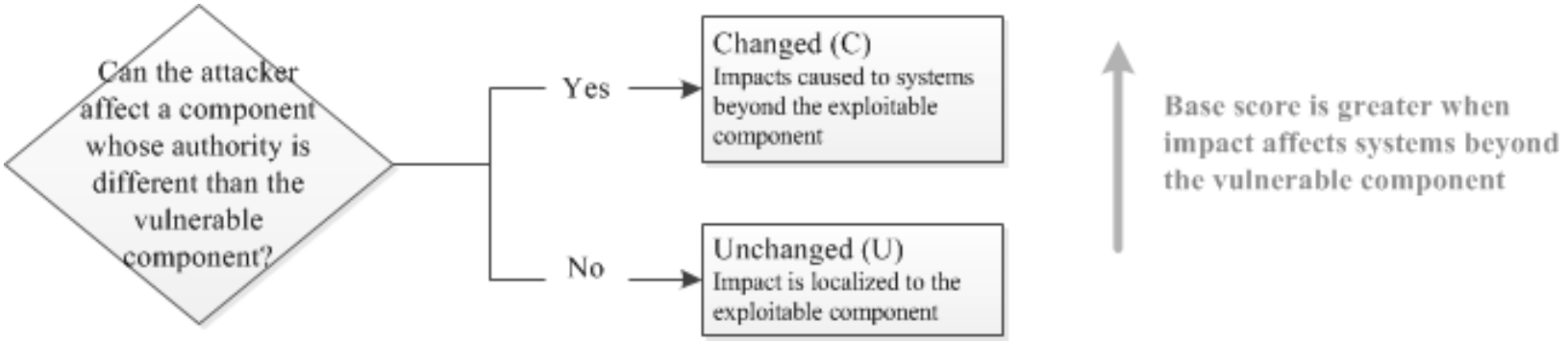
Privileges Required



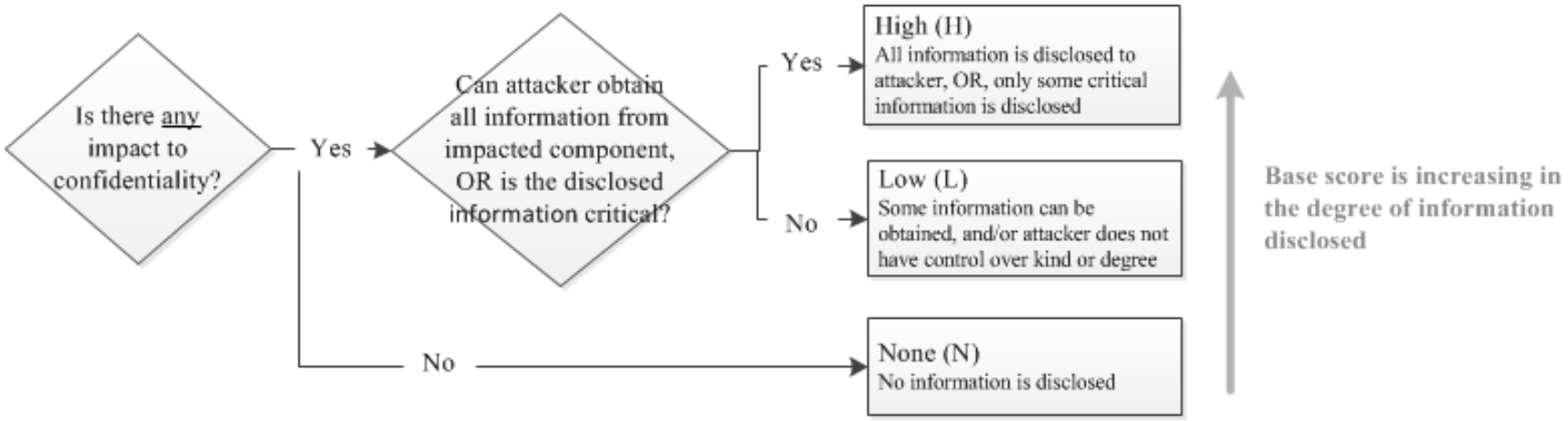
User Interaction



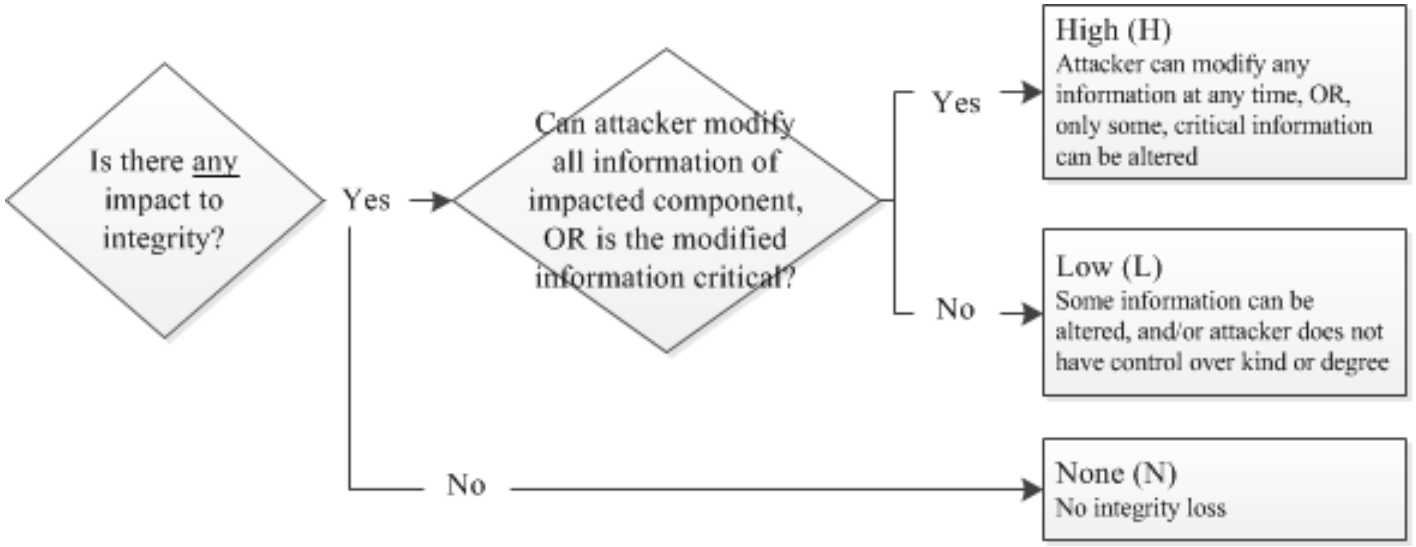
Scope


Can the attacker affect a component whose authority is different than the vulnerable component?
Yes
Changed (C)
Impacts caused to systems beyond the exploitable component
No
Unchanged (U)
Impact is localized to the exploitable component
Base score is greater when impact affects systems beyond the vulnerable component

Confidentiality

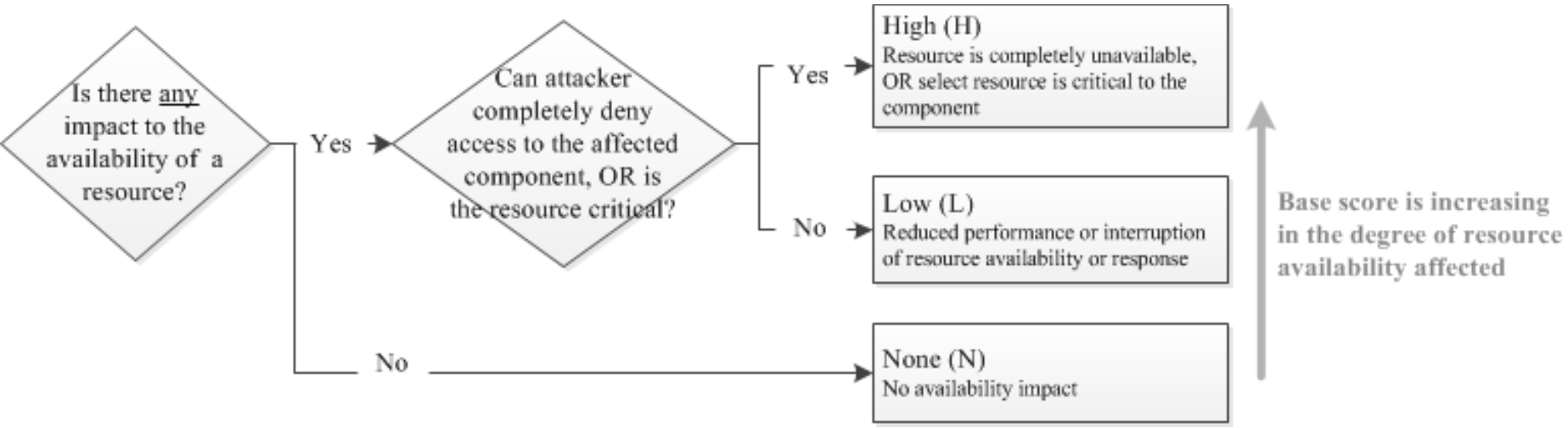


Integrity



Base score is increasing in the degree of information that can be modified

Availability



Vulnerabilities

CVE-2013-1937

phpMyAdmin Reflected Cross-site Scripting Vulnerability		
V2:	4.3	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	P	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2013-0375

MySQL Stored SQL Injection		
V2:	5.5	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	S	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	P	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2014-3566

SSLv3 “POODLE” Vulnerability		
V2:	4.3	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	N	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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 cleartext data via a padding-oracle attack, aka the "POODLE" issue.

CVE-2012-1516

VMware Guest to Host Escape Vulnerability		
V2:	9.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	S	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

Due to a flaw in the handler function for RPC commands, it is possible to manipulate data pointers within the 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.

CVE-2009-0783

Apache Tomcat XML Parser Vulnerability		
V2:	4.6	V3
Access Vector	L	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	P	Scope:
Availability	P	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2012-0384

Cisco IOS Arbitrary Command Execution Vulnerability		
V2:	8.5	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	S	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2015-1098

Apple iWork Denial of Service Vulnerability		
V2:	6.8	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	P	Scope:
Availability	P	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2014-0160

OpenSSL “Heartbleed” Vulnerability		
V2:	5.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	N	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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

GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability		
V2:	10.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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 ENV occurs across a privilege boundary from Bash execution

CVE-2008-1447

DNS Insufficient Socket Entropy Vulnerability AKA “Kaminsky Bug”		
V2:	5.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	P	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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."

CVE-2014-2005

Sophos Login Screen Bypass Vulnerability		
V2:	5.0	V3
Access Vector	L	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2010-0467

Joomla Directory Traversal Vulnerability		
V2:	5.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	N	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2012-1342

Cisco Access Control Bypass Vulnerability		
V2:	5.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	P	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

Cisco Carrier Routing System (CRS) 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.

CVE-2013-6014

Juniper Proxy ARP Denial of Service Vulnerability		
V2:	6.1	V3
Access Vector	A	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	C	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2014-9253

DokuWiki Reflected Cross-site Scripting Attack		
V2:	4.3	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	P	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2009-0658

Adobe Acrobat Buffer Overflow Vulnerability		
V2:	9.3	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2011-1265

Microsoft Windows Bluetooth Remote Code Execution Vulnerability		
V2:	8.3	V3
Access Vector	A	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2014-2019

Apple iOS Security Control Bypass Vulnerability		
V2:	4.9	V3
Access Vector	L	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	N	User Interaction:
Integrity	C	Scope:
Availability	N	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2015-0970

SearchBlox Cross-Site Request Forgery Vulnerability		
V2:	6.8	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	P	Scope:
Availability	P	Confidentiality:
		Integrity:
		Availability:

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 allow 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.

CVE-2014-0224

SSL/TLS MITM Vulnerability		
V2:	6.8	V3
Access Vector	N	Attack Vector:
Access Complexity	M	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	P	User Interaction:
Integrity	P	Scope:
Availability	P	Confidentiality:
		Integrity:
		Availability:

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.

CVE-2012-5376

Google Chrome Sandbox Bypass vulnerability		
V2:	10.0	V3
Access Vector	N	Attack Vector:
Access Complexity	L	Attack Complexity:
Authentication	N	Privileges Required:
Confidentiality	C	User Interaction:
Integrity	C	Scope:
Availability	C	Confidentiality:
		Integrity:
		Availability:

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.

Vulnerability Chaining

Chain of Magento Vulnerabilities

CVSS v3: 9.8

- Online shopping cart, Magento
  - Patched in SUPEE-5344
  - Vulnerabilities described by CheckPoint CPAI-2015-0106-2, -0107, and -0108)
- Complex set of vulnerabilities providing remote SQL injection by unauthorized attackers
- Capable of running any SQL commands, including adding an admin user

SUPEE-5344 Composition

- 3-5 vulnerabilities / exposures
- CVE-2015-1399 / CVE-2015-3458
- OSVDB 121261 (No CVE)
- CVE-2015-3457
- CVE-2015-1398
- CVE-2015-1397

Attacking the Magento Chain

CVE-2015-1399/-3458
4.9

Unauthenticated, remote attackers can specify the 'forwarded' parameter to bypass authorization checks, permitting the execution of any admin module which does not perform further privilege checks

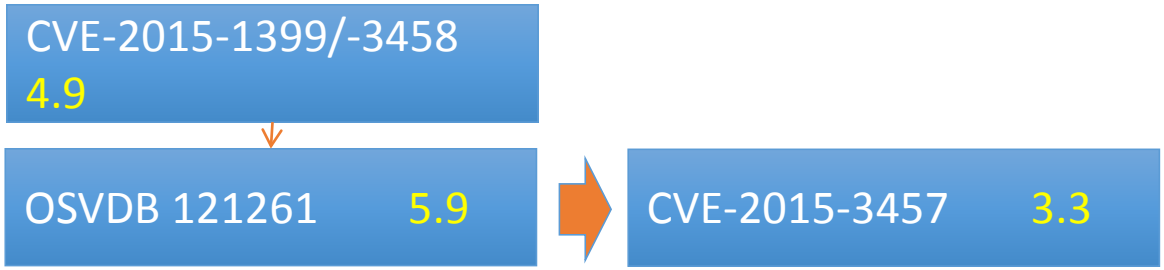
Attacking the Magento Chain

CVE-2015-1399/-3458
4.9

OSVDB 121261 5.9

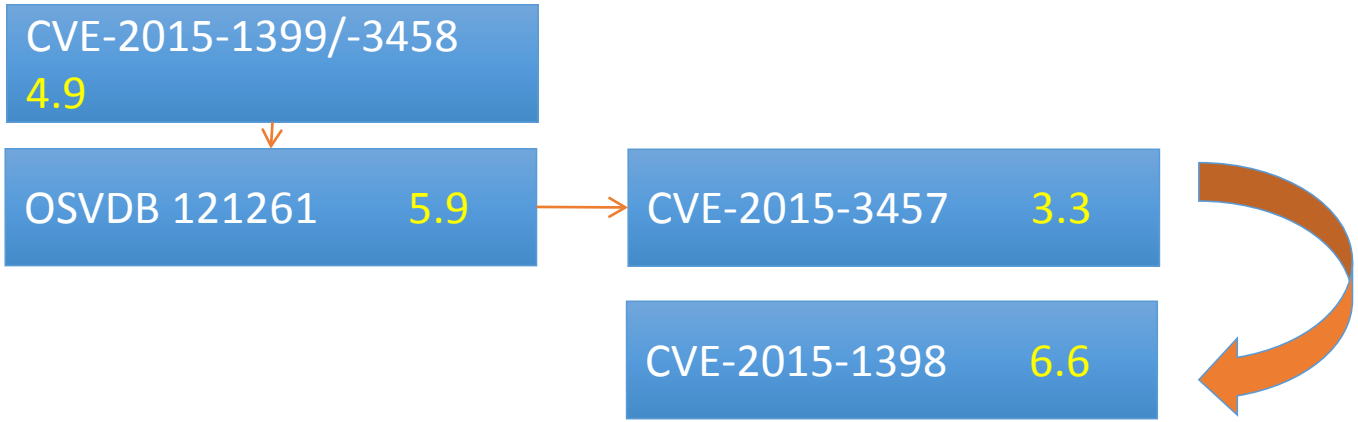
Unauthenticated, remote attackers can specify the ‘forwarded’ parameter to bypass authorization checks, permitting the execution of any admin module which does not perform further privilege checks

Attacking the Magento Chain



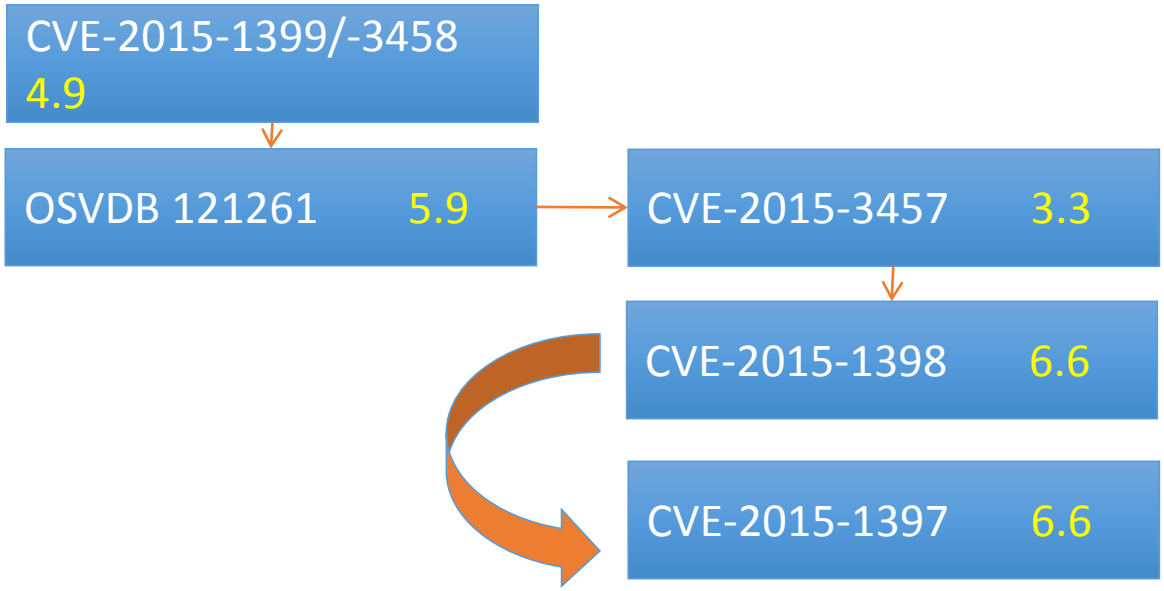
Unauthenticated, remote attackers can create an arbitrary “block” class, which may be called with no arguments; typically responsible for GUI operations

Attacking the Magento Chain



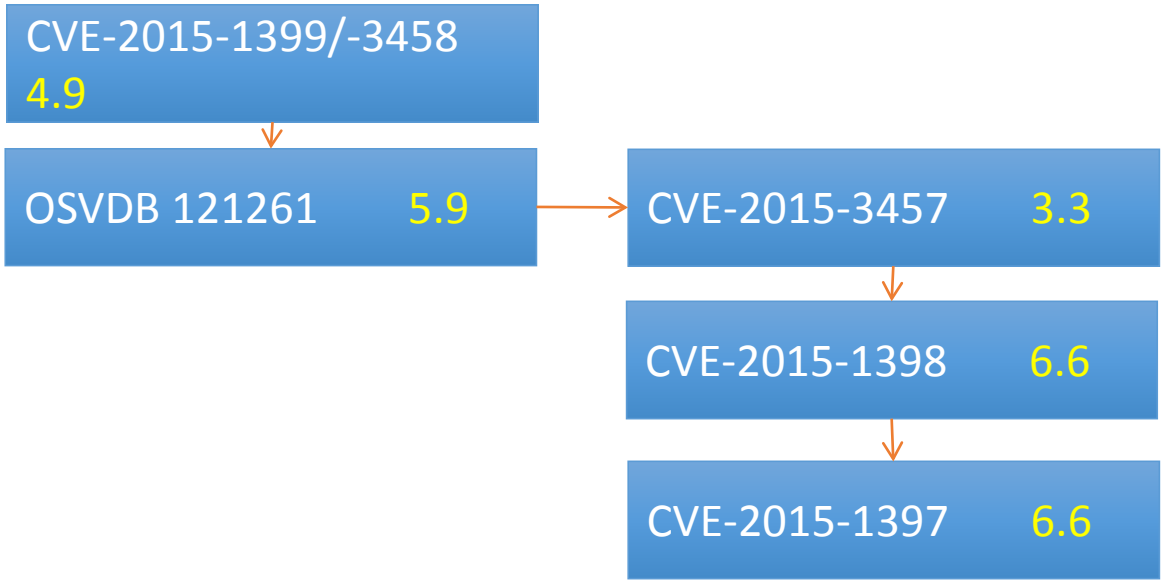
Loads an image and processes through an input filter that has a user-controlled path; Local File Inclusion will call the file with Admin privileges

Attacking the Magento Chain



SQLi from a local csv file, allows arbitrary Command Execution and file creation as an administrator

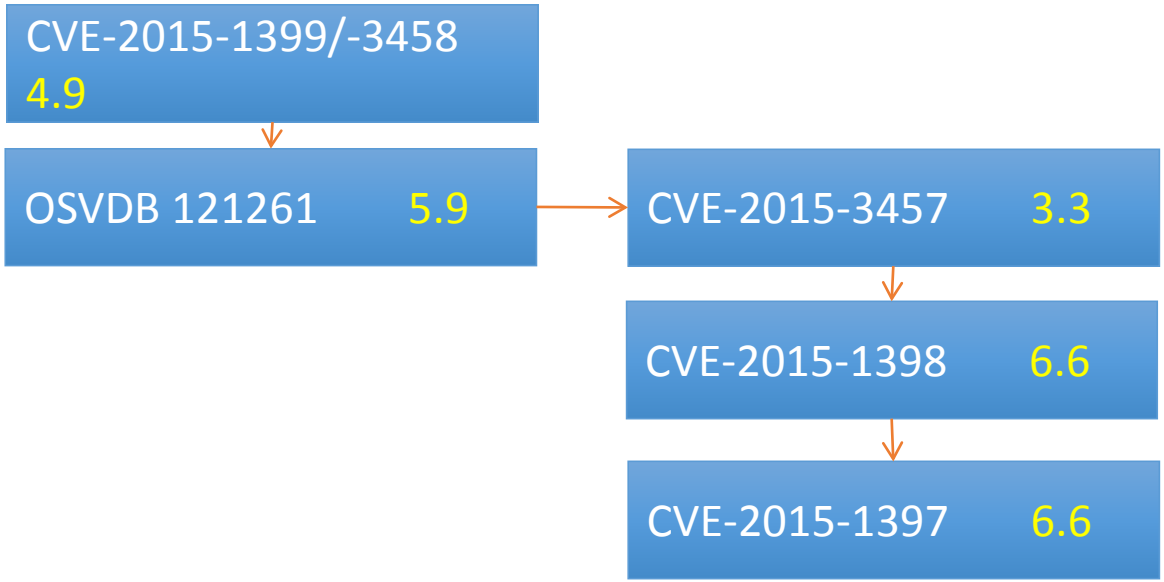
Attacking the Magento Chain



Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

Attacking the Magento Chain

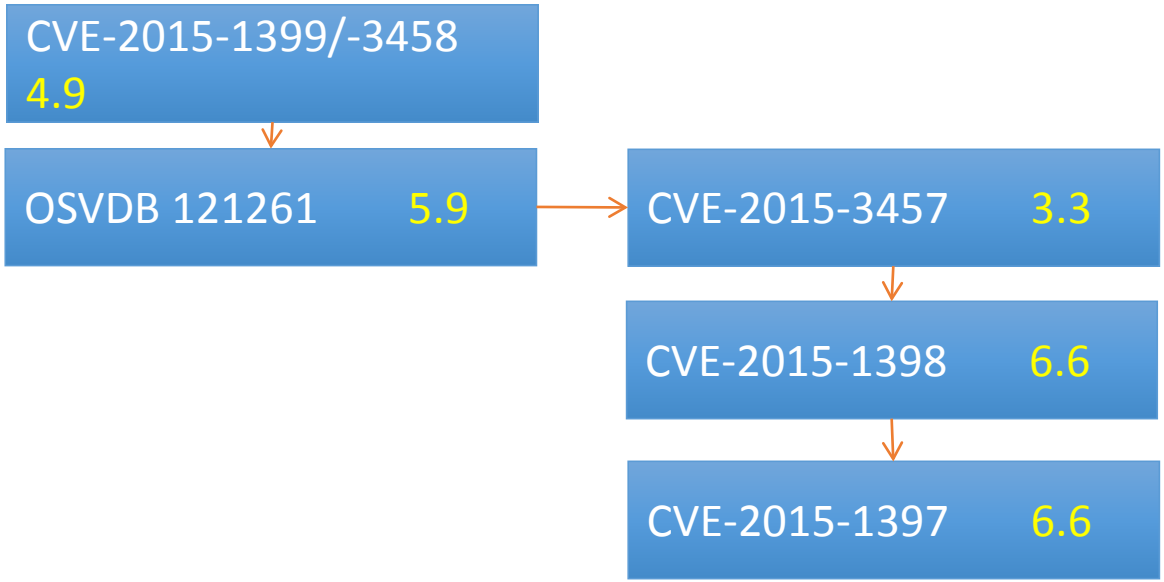


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

CVE-2015-1399 – Remote attacker includes a phar:// archive

Attacking the Magento Chain

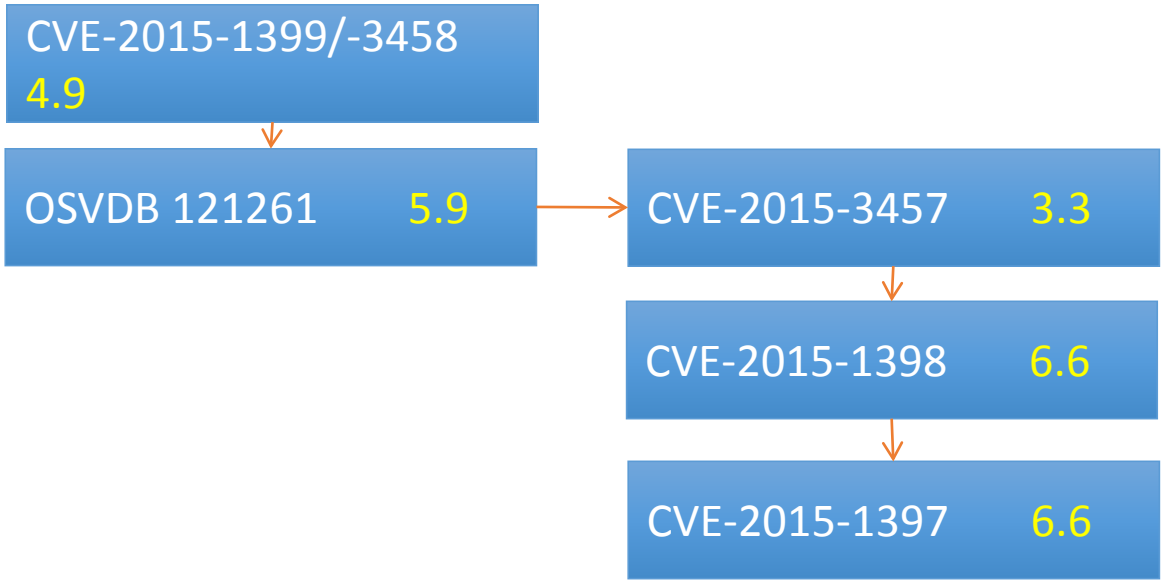


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

CVE-2015-1399 – Remote attacker controls contents of archive / image file

Attacking the Magento Chain

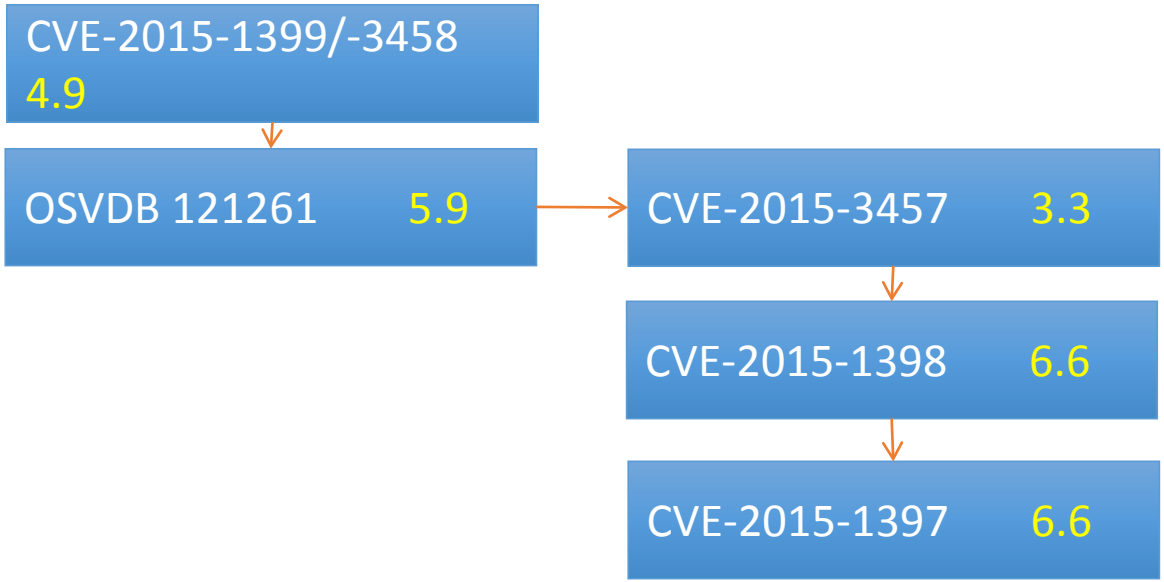


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

OSVDB 121261 – Attacker bypasses authentication via ‘forwarded’ parameter

Attacking the Magento Chain

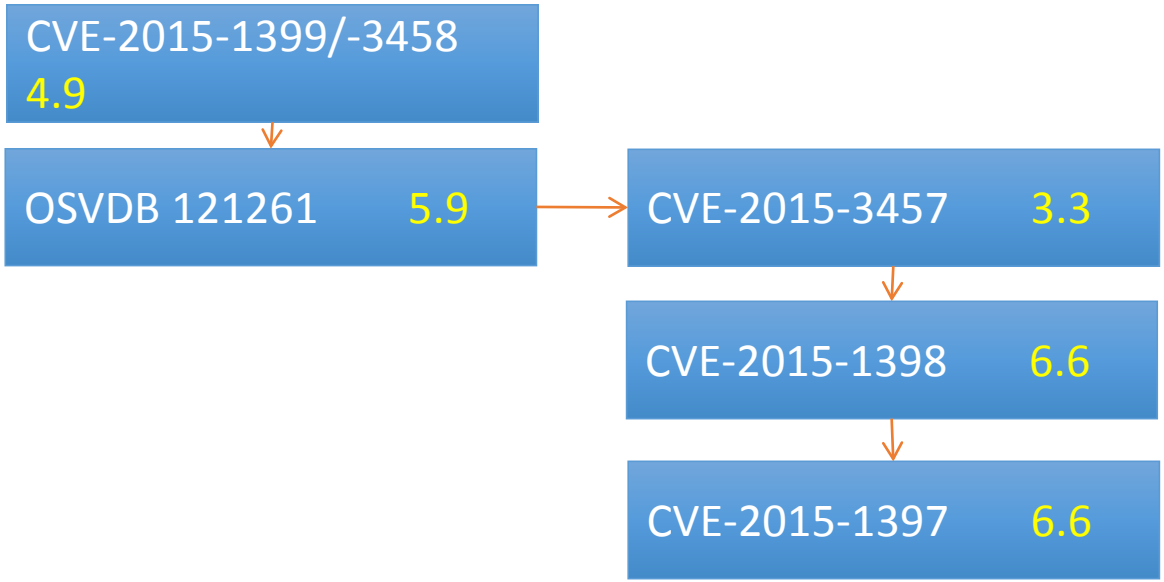


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

User Interaction & Scope are identical across all vulnerabilities

Attacking the Magento Chain

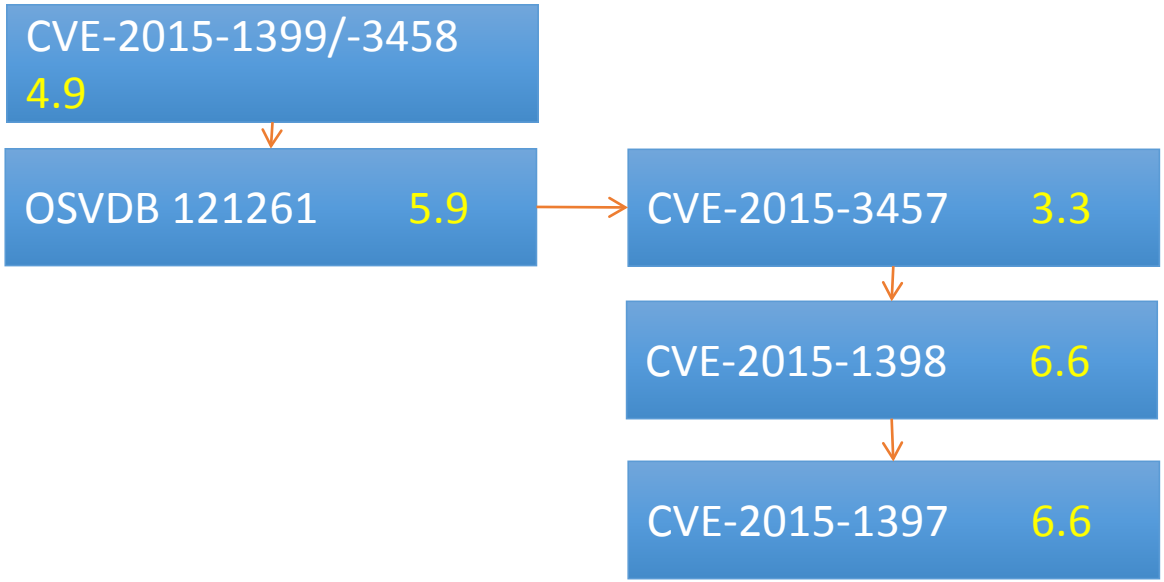


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

CVE-2015-3457 allows the creation of an arbitrary method

Attacking the Magento Chain

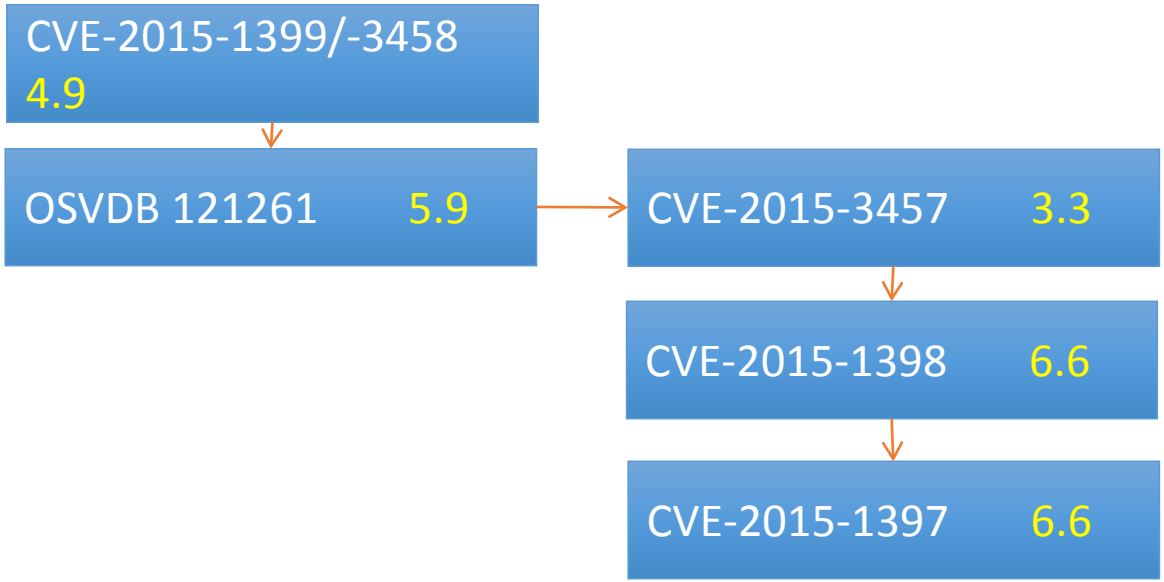


Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

CVE-2015-1398 allows an attacker to include a local image file (placed by -1399) via Cms_Wysiwyg

Attacking the Magento Chain



Chain:
CVE-2015-1399 => OSVDB 121261 => CVE-2015-3457 => CVE-2015-1398 => CVE-2015-1397

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H 9.8

CVE-2015-1397 allows SQLi as Magento administrator from the LFI provided by -1398

CVE-2015-1399 / CVE-2015-3458

Magento setScriptPath() Remote File Inclusion Vulnerability			
V2:	6.5	V3	4.9
Access Vector	N	Attack Vector:	N
Access Complexity	L	Attack Complexity:	L
Authentication	S	Privileges Required:	H
Confidentiality	P	User Interaction:	N
Integrity	P	Scope:	U
Availability	P	Confidentiality:	N
		Integrity:	H
		Availability:	N

Magento contains a flaw that is due to the setScriptPath() function in the Mage_Core_Block_Template_Zend class not properly sanitizing user-supplied input before returning it to the user. This may allow a remote attacker to include a file from a remote host that contains commands or code that will be executed by the vulnerable script with the same privileges as the web server.

No CVE (OSVDB 121261)

Magento requestedActionName Authentication Bypass			
V2:	5.0	V3	5.9
Access Vector	N	Attack Vector:	N
Access Complexity	L	Attack Complexity:	H
Authentication	N	Privileges Required:	N
Confidentiality	N	User Interaction:	N
Integrity	P	Scope:	U
Availability	N	Confidentiality:	H
		Integrity:	N
		Availability:	N

Magento contains a flaw in requestedActionName that is triggered during the handling of forwarded parameters. This may allow a remote attacker to bypass controller request authentication mechanisms.

CVE-2015-3457

Magento Unauthorized Invocation of setDataUsingMethod() function		
V2:	V3	3.3
Access Vector	Attack Vector:	N
Access Complexity	Attack Complexity:	H
Authentication	Privileges Required:	H
Confidentiality	User Interaction:	N
Integrity	Scope:	U
Availability	Confidentiality:	L
	Integrity:	L
	Availability:	N

Magento contains a flaw that is due to the program failing to restrict users from invoking the setDataUsingMethod() function. This may allow allow an attacker to use blockDirective() to call arbitrary methods without arguments.

CVE-2015-1398

Magento filter() Local File Inclusion Vulnerability			
V2:	6.5	V3	6.6
Access Vector	N	Attack Vector:	N
Access Complexity	L	Attack Complexity:	H
Authentication	S	Privileges Required:	H
Confidentiality	P	User Interaction:	N
Integrity	P	Scope:	U
Availability	P	Confidentiality:	H
		Integrity:	H
		Availability:	H

Magento contains a local file inclusion (LFI) flaw due to the filter() function in cms/adminhtml_template_filter using user-supplied input when crafting the path for a file to include. With a specially crafted request, a remote attacker can include arbitrary files from the targeted host. This may allow disclosing file contents or executing files like PHP scripts. Such attacks are limited due to the script only calling files already on the target host.

CVE-2015-1397

Magento Block Report Search Grid SQL Injection			
V2:	6.5	V3	6.6
Access Vector	N	Attack Vector:	N
Access Complexity	L	Attack Complexity:	H
Authentication	S	Privileges Required:	H
Confidentiality	P	User Interaction:	N
Integrity	P	Scope:	U
Availability	P	Confidentiality:	H
		Integrity:	H
		Availability:	H

Magento contains a flaw that may allow carrying out an SQL injection attack. The issue is due to the Mage_Adminhtml_Block_Report_Search_Grid class not properly sanitizing user-supplied input to the 'popularity' parameter. This may allow a remote attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.