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.

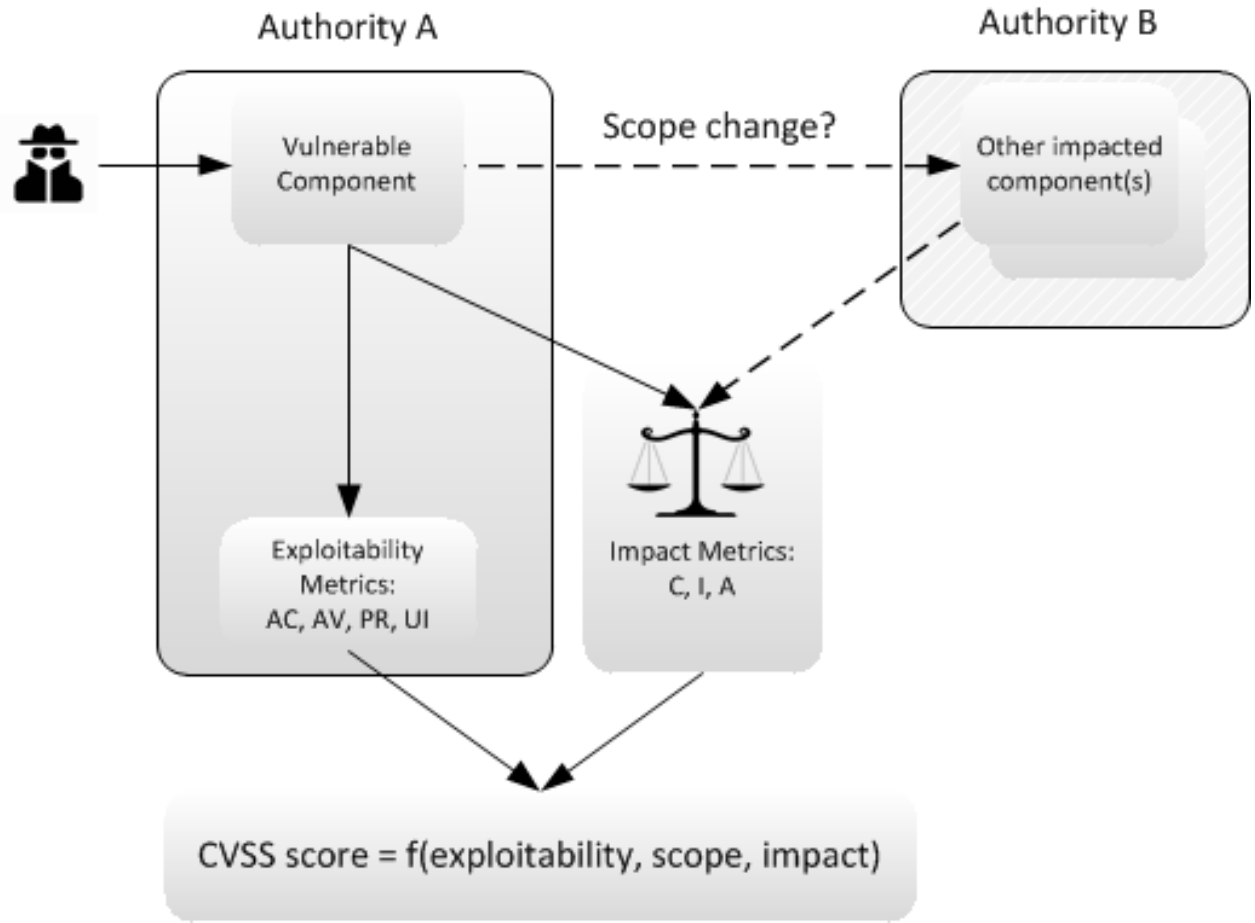
User Interaction

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.

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.

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.

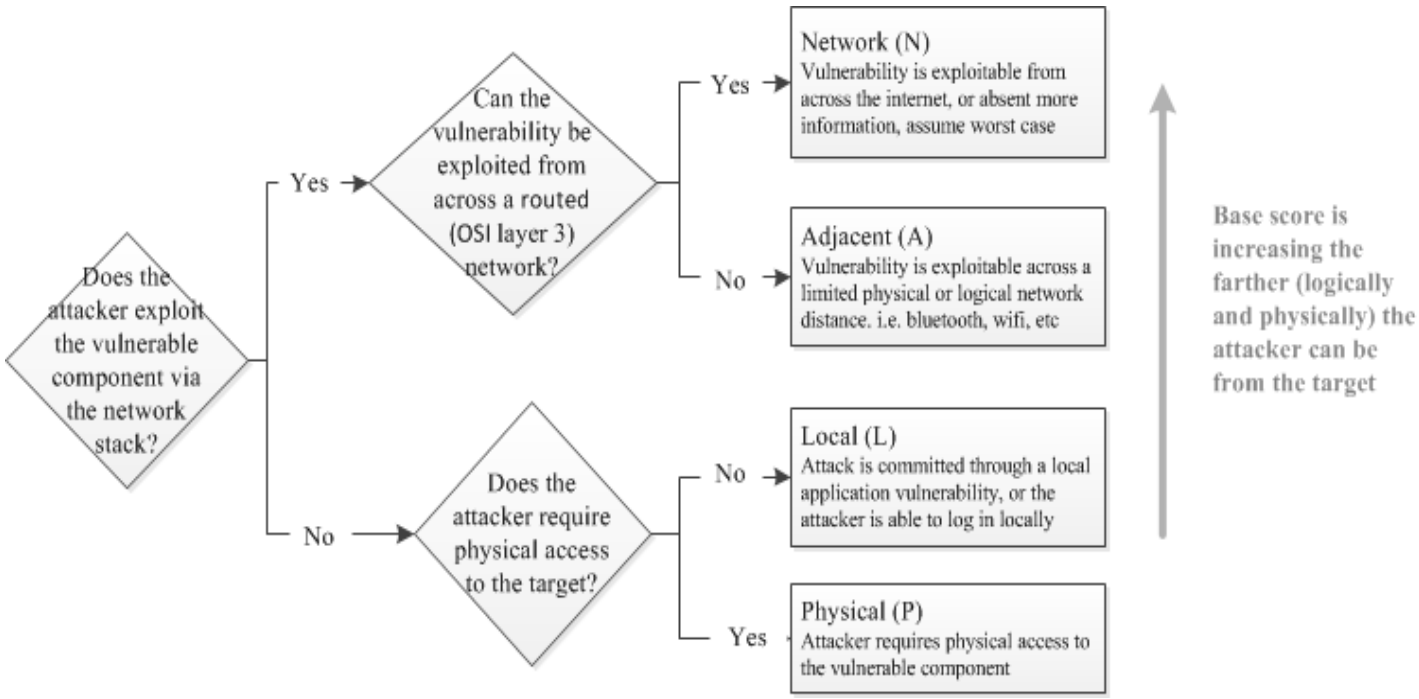
Version 2.0	Version 3.0
Impact metrics reflected percentage of impact caused to a vulnerable application.	Impact metric values now reflect degree of impact, and renamed to “none,” “low,” and “high.”
The Environmental metrics of Target Distribution and Collateral Damage potential were not found to be 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



Vulnerabilities

CVE-2013-1937

phpMyAdmin Reflected Cross-site Scripting Vulnerability			
V2:	4.3	V3	Score:
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.