


UNIVERSITY
OF TRENTO - Italy




Cyber Security Risk Assessment Spring 2018

Lecture 10


Quantitative Risk Analysis

Scoring Vulnerabilities

16/04/18 Fabio Massacci - CyberRisk Assessment 1



UNIVERSITY
OF TRENTO - Italy




Recall: qualitative vs quantitative

From lecture 05, slide 25

Threat Source	Threat Event	Impact
Alice	Install Malware	Moderate
Outsider	SQL Injection	High

- **Qualitative assessment**
 - Malware has a lower impact than SQLi → assigned based on expert judgment
- **Result:**
 - First fix SQL injection because it has a high impact
 - Confidentiality and Integrity impacts on data
 - Then add controls for malware (update AV, data caps policies,..)
 - Worrisome but moderated impact
 - Disclosure of only some data/compartmentalization

16/04/18 Fabio Massacci - CyberRisk Assessment 2

UNIVERSITY OF TRENTO - Italy 

Recall: qualitative vs quantitative

- ***Is this always reasonable?***
 - Should Christine Patch ALL SQLi vulnerabilities on ALL software?
 - Can not know without a technical/objective analysis of the vulnerability/threat

Vulnerability Summary for CVE-2016-2174

Original release date: 06/13/2016
 Last revised: 06/14/2016
 Source: US-CERT/NIST


Overview

SQL injection vulnerability in the policy admin tool in Apache Ranger before 0.5.3 allows remote authenticated administrators to execute arbitrary SQL commands via the eventTime parameter to service/plugins/policies/eventTime.

Vulnerability Summary for CVE-2016-8582

A vulnerability exists in gauge.php of AlienVault OSSIM and USM before 5.3.2 that allows an attacker to execute an arbitrary SQL query and retrieve database information or read local system files via MySQL's LOAD_FILE.


16/04/18 Fabio Massacci - CyberRisk Assessment 3

UNIVERSITY OF TRENTO - Italy 


Vulnerabilities

- ***A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy***
Definition from NIST SP 800-30
- **Software vulnerabilities**
 - Buffer overflows
 - Authentication
 - Privilege escalation
 - XSS
 - SQL Injection
 - etc

16/04/18 Fabio Massacci - CyberRisk Assessment 4




UNIVERSITY OF TRENTO - Italy




Why to grade vulnerabilities?

- **Central question:**
 - **How severe are the security problems affecting my software and database configuration?**
 - To fix a problem you must 1) realize that you have a problem and 2) understand how big the problem is
- **Not all vulnerabilities are the same**
 - Vulnerability counting can NOT be a measure of severity
 - What is the threat level of your systems?
 - Clients and users should be informed too
 - Not all users are “security experts”
 - “IT knowledge” can be assumed
 - How to **measure and communicate** a security issue?

16/04/18 Fabio Massacci - CyberRisk Assessment 5




UNIVERSITY OF TRENTO - Italy




Usage in Practice

- **PCI-DSS v2 (June 2012) – Credit Card Software Standard**
 - “Risk rankings should be based on industry best practices. For example, criteria for ranking —High risk vulnerabilities may include a **CVSS base score** of 4.0 or above”
 - **If your merchant software has a vulnerability that is high risk and you get a credit card fraud, Visa and Mastercard will not pay...**
- **NIST SCAP Protocol v1.2 (Draft Jan 2012)**
 - “Organizations should use **CVSS base scores** to assist in prioritizing the remediation of known security-related software flaws based on the relative severity of the flaws.”
- **Several Databases Exists to collect vulnerabilities**
 - NVD – National (US) Vulnerability Database
 - The US version but used by almost everybody else.
 - CNNVD – Chinese version of Vulnerability Database
 - Sometimes faster than the US database in reporting vulnerabilities, sometimes slower.

16/04/18 Fabio Massacci - CyberRisk Assessment 6




UNIVERSITY OF TRENTO




The Common Vulnerability Scoring System

- **CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities**
- **Goal is to have a *shared system of metrics* to analyze and measure vulnerabilities**
 - Different users score the same vuln in the same way → **severity assessment**
 - Different people “read” the same vuln and understand the same thing → **severity communication**

16/04/18 Fabio Massacci - CyberRisk Assessment 7



UNIVERSITY OF TRENTO - Italy



CVSS v(x) walkthrough

- **CVSS v(1) introduced back in 2004 by First.org**
 - Reception was good but implementation was confusing
 - Not peer-reviewed
- **CVSS v(2) workings started in 2005, released in 2007**
 - Peer-reviewed, industry feedback
 - Became *standard-de-facto* vulnerability scoring system in the industry
- **CVSS v(3) workings started in 2012, released in 2015**
 - Builds on top of v2
 - Changes the “scoring philosophy”
 - Further step toward a precise scoring system

16/04/18 Fabio Massacci - CyberRisk Assessment 8

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

CVSS v3

<http://www.first.org/cvss/v3/development>

- **CVSS is based on three metric groups**

Base Metric Group

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope
- Impact Metrics (Confidentiality, Integrity, Availability)

Temporal Metric Group

- Exploitability
- Remediation Level
- Report Confidence

Environmental Metric Group

- Mitigated Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Base Metrics $f(x_1, x_2, \dots, x_n)$ Temporal Metrics $f(y_1, y_2, \dots, z_n)$ Environmental Metrics $f(z_1, z_2, \dots, z_n)$

Score Vector CVSS

16/04/18 9

Fabio Massacci - CyberRisk Assessment

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

CVSS Base metric overview

- **Exploitability metrics**
 - Attack Vector
 - Attack Complexity
 - User Interaction
 - Privileges Required


Measured over the vulnerable component
- **Scope metric**

Auth. Authority of Vulnerable Component = Auth. Authority of Impacted Component?
- **Impact metrics**
 - Confidentiality
 - Integrity
 - Availability


Measured over the impacted component

16/04/18 10

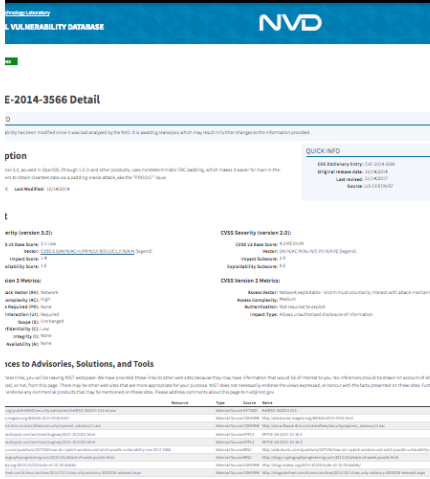
Fabio Massacci - CyberRisk Assessment



UNIVERSITY OF TRENTO - Italy



CVSS May Be Already Known




- **National (US) Vulnerability Database**
 - <https://nvd.nist.gov>
 - <https://cve.mitre.org>
- **May include several mitigation measures**
- **But this is only true for very popular software**
 - YOUR software might not be there...


16/04/18

Fabio Massacci - CyberRisk Assessment

11



UNIVERSITY OF TRENTO - Italy



Scoring example


- **You work in the PSIRT of a firewall vendor.**
 - PSIRT = Product Security Incident Response Team
- **You sell the product to a web-sites doing online commerce → your company must prioritize work based on CVSS scores**
- **WHAT HAPPENED (1)**
 - A security researcher sends details of a vulnerability they have found in one of your firewall products.
 - The vulnerability allows attackers to bypass authentication to the firewall's admin panel when the default "defrag packets before forward" flag is disabled, due to a faulty management of invalid fragmented IP datagrams.
- **WHAT YOU DO (1)**
 - calculate a CVSS Base Score based on the researcher's report, to rate the severity of the vulnerability.

AV, AC, UI, PR, S, C, I, A
- **OK but how do I do it? → this lecture**


16/04/18

Fabio Massacci - CyberRisk Assessment

12




UNIVERSITY OF TRENTO - Italy




Expl. Metrics: Attack Vector

- **This metric reflects the context in which the vulnerability exploitation occurs.**
- **The more remote an attacker (or the attack) can be from the target, the greater the vulnerability score.**
- **Possible values:**
 1. **Network:** exploitation is just bound to the network stack
 2. **Adjacent Network:** attacker needs to be in same subnet
 3. **Local:** attack is not bound to network stack, but rather to I/O on system. In some cases, the attacker may be logged in locally in order to exploit the vulnerability, otherwise, she may rely on User Interaction to execute a malicious file.
 4. **Physical:** attacker must be physically operating over the vulnerable component

16/04/18 Fabio Massacci - CyberRisk Assessment 13




UNIVERSITY OF TRENTO - Italy




Expl. Metrics: Attack Complexity

- **This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.**
- **Possible values:**
 1. **High:** A successful attack depends on conditions outside the attacker's control. That is, a successful attack cannot be accomplished, 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.
 2. **Low:** Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable exploit success against a vulnerable target

16/04/18 Fabio Massacci - CyberRisk Assessment 14




UNIVERSITY OF TRENTO - Italy




Examples for Attack Complexity: High

- ***For example, a successful attack may depend on an attacker overcoming any of the following conditions:***
 - The attacker must conduct **target-specific reconnaissance**. For example, on target configuration settings, sequence numbers, shared secrets, etc.
 - The attacker must **prepare the target environment** to improve exploit reliability. For example, repeated exploitation to win a race condition, or overcoming advanced exploit mitigation techniques.
 - The attacker **injects herself into the logical network path** between the target and the resource requested by the victim in order to read and/or modify network communications (e.g. man in the middle attack).

16/04/18 Fabio Massacci - CyberRisk Assessment 15




UNIVERSITY OF TRENTO - Italy




Expl. Metrics: Privileges Required

- ***This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.***
- ***Possible values:***
 1. **High**: 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.
 2. **Low**: 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.
 3. **None**: The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files to carry out an attack.

16/04/18 Fabio Massacci - CyberRisk Assessment 16




UNIVERSITY OF TRENTO - Italy




Expl. Metrics: User Interaction

- ***This metric captures the requirement for a user, other than the attacker, to participate in the successful compromise the vulnerable component.***
- ***This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user-initiated process) must participate in some manner.***
- ***Possible values:***
 1. **Required**: 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.
 2. **None**: The vulnerable system can be exploited without any interaction from any user.

16/04/18 Fabio Massacci - CyberRisk Assessment 17



UNIVERSITY OF TRENTO - Italy



Impact metrics

- ***Measures the losses on***
 - **Confidentiality**, → impact on confidentiality of **data**
 - *property that information is not made available or disclosed to unauthorized individuals, entites, or processes*
 - **Integrity**, → impact on integrity of **data**
 - *the “property of accuracy and completeness” of information*
 - **Availability** → impact on availability of **the component**
 - *is the “property of being accessible and usable upon demand by an unauthorized entity”*
- ***Each metric measures the losses suffered by the impacted component***
- ***Possible values:***
 1. **High** → total loss
 2. **Low** → partial loss
 3. **None** → no loss

16/04/18 Fabio Massacci - CyberRisk Assessment 18

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Individual Values are Aggregated

7.6
(High)

Base Score

Attack Vector (AV)

Network (N) Adjacent (A) Local (L)

Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)


16/04/18 Fabio Massacci - CyberRisk Assessment 19

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL


Qualitative ratings of Global CVSS

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

16/04/18 Fabio Massacci - CyberRisk Assessment 20



UNIVERSITY OF TRENTO - Italy




Scoring Guide/Philosophy

- **Attack Vector** → *is the attack bound to the network stack?*
- **Attack Complexity** → *can the attacker control all factors relevant to the exploitation?*
- **Privileges Required** → *does the attacker need be authenticated?*
- **User Interaction** → *does the victim user need to interact with the attack?*
- **Scope** → *is the authorisation authority under which the vulnerable component is the same as the impacted component?*
- **Impact**
 - Confidentiality, Integrity → Data
 - Availability → Service
- **Scoring rule: When more than one assessment is possible, go with the more severe one**
 - e.g. exploitation can happen both though local I/O and on network stack → go with network


16/04/18

Fabio Massacci - CyberRisk Assessment

21



UNIVERSITY OF TRENTO - Italy




You may have noticed.. From 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 <i>thing suffering the impact</i> (the impacted component) is different from <i>the thing that is vulnerable</i> (the vulnerable component).
Access Vector may conflate attacks that require local system access and physical hardware attacks.	Local and Physical values are now separated in the Attack Vector metric.
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).


16/04/18

Fabio Massacci - CyberRisk Assessment

22




UNIVERSITY OF TRENTO - Italy




From v2.0 to v3.0

Version 2.0	Version 3.0
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.
Impact metrics reflected percentage of impact caused to a vulnerable application.	Impact metric values now reflect the degree of impact, and are 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.

16/04/18 Fabio Massacci - CyberRisk Assessment 23



UNIVERSITY OF TRENTO - Italy




Scoring example (again)


- **You work in the PSIRT of a firewall vendor.**
 - PSIRT = Product Security Incident Response Team
- **Your company prioritizes work based on CVSS scores.**
- **WHAT HAPPENED (1)**
 - A security researcher sends details of a vulnerability they have found in one of your firewall products.
 - The vulnerability allows attackers to bypass authentication to the firewall's admin panel when the default "defrag packets before forward" flag is disabled, due to a faulty management of invalid fragmented IP datagrams.
- **WHAT YOU DO (1)**
 - calculate a CVSS Base Score based on the researcher's report, to rate the severity of the vulnerability.

AV, AC, UI, PR, S, C, I, A

16/04/18 Fabio Massacci - CyberRisk Assessment 24



UNIVERSITY OF TRENTO - Italy



Scoring calculator

Base Score

9.8
(Critical)

Attack Vector (AV)

Network (N) Adjacent (A)

Attack Complexity (AC)

Local Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)


None (N) Low (L) High (H)

Local 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). Such a vulnerability is often termed "remotely exploitable" and can be thought of as an attack being exploitable one or more network hops away.


16/04/18

Fabio Massacci - CyberRisk Assessment

25



UNIVERSITY OF TRENTO - Italy



Scoring Exercise (Class)


- **MS Word Denial-of-Service 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.

Attack Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Confidentiality	
Integrity	
Availability	


16/04/18

Fabio Massacci - CyberRisk Assessment

26



UNIVERSITY OF TRENTO - Italy



Scoring Exercise (correct)


- **MS Word Denial-of-Service 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.

Attack Vector	Local
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Confidentiality	None
Integrity	None
Availability	High


16/04/18

Fabio Massacci - CyberRisk Assessment

27



UNIVERSITY OF TRENTO - Italy



Overall Score

Base Score

5.5

(Medium)

Attack Vector (AV)

Network (N) Adjacent (A)

Local (L) Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) **Required (R)**

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) High (H)

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) **High (H)**

16/04/18

Fabio Massacci - CyberRisk Assessment

28

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

What if it was really over the network?

Base Score
7.5
(High)

<p>Attack Vector (AV)</p> <p>Network (N) Adjacent (A)</p> <p>Local (L) Physical (P)</p> <p>Attack Complexity (AC)</p> <p>Low (L) High (H)</p> <p>Privileges Required (PR)</p> <p>None (N) Low (L) High (H)</p> <p>User Interaction (UI)</p> <p>None (N) Required (R)</p>	<p>Scope (S)</p> <p>Unchanged (U) Changed (C)</p> <p>Confidentiality (C)</p> <p>None (N) Low (L) High (H)</p> <p>Integrity (I)</p> <p>None (N) Low (L) High (H)</p> <p>Availability (A)</p> <p>None (N) Low (L) High (H)</p>
---	---

16/04/18
Fabio Massacci - CyberRisk Assessment
29

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Scoring Exercise (class)

- **SSLv3 POODLE Vulnerability (CVE-2014-3566)**
 - 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 Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Confidentiality	
Integrity	
Availability	

16/04/18
Fabio Massacci - CyberRisk Assessment
30

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Scoring Exercise (correct)

- **SSLv3 POODLE Vulnerability (CVE-2014-3566)**
 - 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 Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required (?)
Confidentiality	Low
Integrity	None
Availability	None

16/04/18 Fabio Massacci - CyberRisk Assessment 31


UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Scoring Exercise (class)


- **Apache Tomcat XML Parser 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.

Attack Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Confidentiality	
Integrity	
Availability	

16/04/18 Fabio Massacci - CyberRisk Assessment 32



UNIVERSITY
OF TRENTO - Italy



Scoring Exercise (correct)


- **Apache Tomcat XML Parser 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.

Attack Vector	Local
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Confidentiality	Low
Integrity	Low
Availability	Low


16/04/18

Fabio Massacci - CyberRisk Assessment

33



UNIVERSITY
OF TRENTO - Italy



Scoring Exercise (class)

- **Apple iWork Denial of Service Vulnerability (CVE-2015-1098)**
 - 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 Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Confidentiality	
Integrity	
Availability	

16/04/18

Fabio Massacci - CyberRisk Assessment

34

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Scoring Exercise (correct)

- **Apple iWork Denial of Service Vulnerability (CVE-2015-1098)**
 - 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 Vector	Local
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Confidentiality	High
Integrity	High
Availability	High

16/04/18 Fabio Massacci - CyberRisk Assessment 35


UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Scoring Exercise (class)


- **CISCO Devices Privileges escalation (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.

Attack Vector	
Attack Complexity	
Privileges Required	
User Interaction	
Confidentiality	
Integrity	
Availability	High

16/04/18 Fabio Massacci - CyberRisk Assessment 36



UNIVERSITY
OF TRENTO - Italy



Scoring Exercise (correct)


- **CISCO Devices Privileges escalation (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.

Attack Vector	Network
Attack Complexity	High
Privileges Required	Low
User Interaction	None
Confidentiality	High
Integrity	High
Availability	High


16/04/18

Fabio Massacci - CyberRisk Assessment

37



UNIVERSITY
OF TRENTO - Italy




Scoring exercise (Friday)

- **Spreadsheet with 30 vulnerability descriptions**
 - To be graded according to CVSS v3 guidelines
 - Use the metric description printout for your full reference
- **Please indicate your name and surname on top of the sheet**
- **Fill in:**
 - CVSS v3 metrics
 - **Estimated score:** 1-10 with 10 very bad, 1 not so bad
 - **Confident?** Yes=the vuln is clear to me; No= I'm not sure
 - **Domain knowledge:** Have you ever heard of the software before? Y/N
 - **Comments:** Any comment on the vulnerability. Was the provided information enough?


16/04/18

Fabio Massacci - CyberRisk Assessment

38




UNIVERSITY
OF TRENTO - Italy




Scoring Guide/Philosophy

- **Attack Vector** → *is the attack bound to the network stack?*
 - Network, Adjacent, Local, Physical
- **Attack Complexity** → *can the attacker control all factors relevant to the exploitation?*
 - Low, High
- **Privileges Required** → *does the attacker need be authenticated?*
 - None, Low, High
- **User Interaction** → *does the victim user need to interact with the attack?*
 - None, Required
- **Impact**
 - Confidentiality, Integrity → Data
 - Availability → Service
 - High, Low, None
- **Scoring rule:** *When more than one assessment is possible, go with the more severe one*

16/04/18 Fabio Massacci - CyberRisk Assessment 39



UNIVERSITY
OF TRENTO - Italy



SCOPE METRIC

16/04/18 Fabio Massacci - CyberRisk Assessment 40

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

CVSS v3

<http://www.first.org/cvss/v3/development>

- **CVSS is based on three metric groups**

The diagram illustrates the three metric groups of CVSS v3 and how they contribute to the final score and vector. The **Base Metric Group** includes Attack Vector, Scope (highlighted with a red box), Attack Complexity, Privileges Required, User Interaction, and Impact Metrics (Confidentiality, Integrity, Availability). The **Temporal Metric Group** includes Exploitability, Remediation Level, and Report Confidence. The **Environmental Metric Group** includes Mitigated Base Metrics, Confidentiality Requirement, Integrity Requirement, and Availability Requirement. Below, a flowchart shows the Base Metrics $f(x_1, x_2, \dots, x_n)$, Temporal Metrics $f(y_1, y_2, \dots, y_n)$, and Environmental Metrics $f(z_1, z_2, \dots, z_n)$ (labeled as Optional) contributing to the final CVSS Score and Vector. A thermometer icon indicates the Score (0-10) and a document icon indicates the Vector.

16/04/18

Fabio Massacci - CyberRisk Assessment

41

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

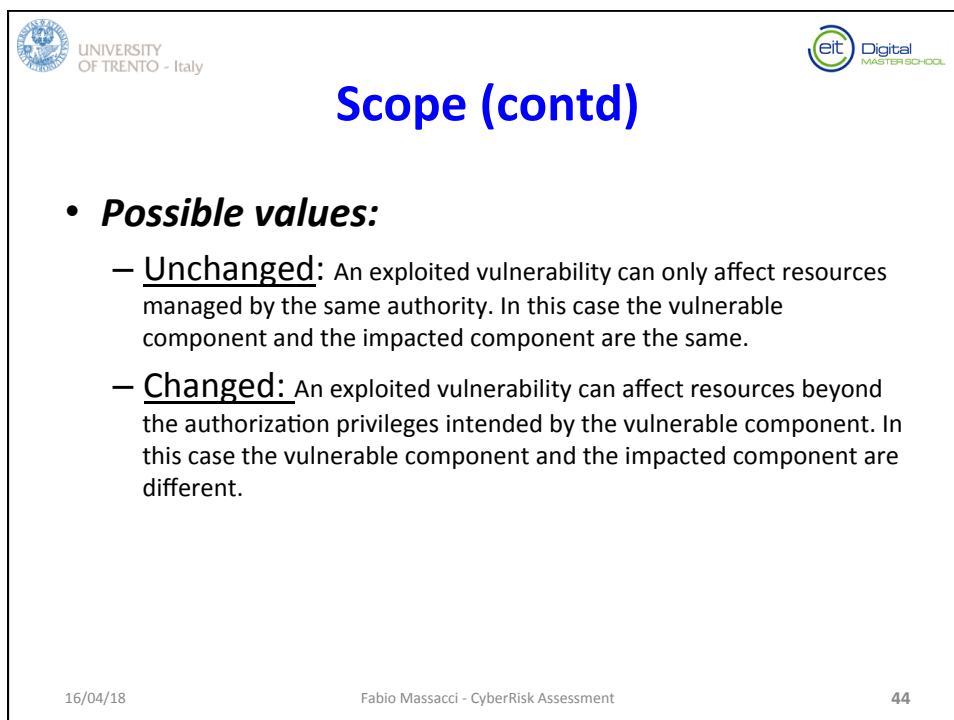
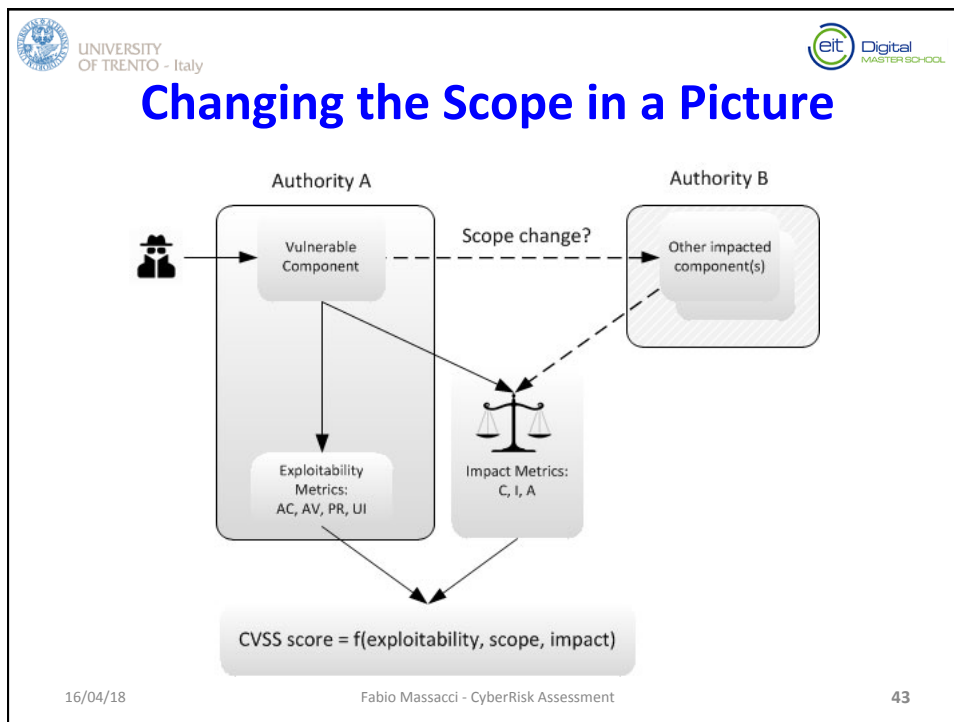
Scope (1)

- **Scope refers to the collection of privileges defined by a computing authority (e.g. an application, an operating system, or a sandbox environment) when granting access to computing resources (e.g. files, CPU, memory, etc). These privileges are assigned based on some method of identification and authorization.**
- **When the vulnerability of a software component governed by one authorization scope is able to affect resources governed by another authorization scope, a Scope change has occurred.**

16/04/18

Fabio Massacci - CyberRisk Assessment

42



UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Effect of scope

What do you expect the final score to go? Up or down? → **7.6 (High) ?**

Base Score

<p>Attack Vector (AV)</p> <p><input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L)</p> <p><input type="radio"/> Physical (P)</p> <p>Attack Complexity (AC)</p> <p><input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>Privileges Required (PR)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>User Interaction (UI)</p> <p><input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)</p>	<p>Scope (S)</p> <p><input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)</p> <p>Confidentiality (C)</p> <p><input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)</p> <p>Integrity (I)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>Availability (A)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p>
--	--

16/04/18 Fabio Massacci - CyberRisk Assessment 45

UNIVERSITY OF TRENTO - Italy eit Digital MASTER SCHOOL

Effect of scope


It goes up because the impact may be suffered by a multitude of non-vulnerable systems

Base Score


9.1 (Critical)

<p>Attack Vector (AV)</p> <p><input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L)</p> <p><input type="radio"/> Physical (P)</p> <p>Attack Complexity (AC)</p> <p><input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>Privileges Required (PR)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>User Interaction (UI)</p> <p><input checked="" type="radio"/> None (N) <input type="radio"/> Required (R)</p>	<p>Scope (S)</p> <p><input type="radio"/> Unchanged (U) <input checked="" type="radio"/> Changed (C)</p> <p>Confidentiality (C)</p> <p><input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)</p> <p>Integrity (I)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p> <p>Availability (A)</p> <p><input type="radio"/> None (N) <input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)</p>
--	--

16/04/18 Fabio Massacci - CyberRisk Assessment 46



UNIVERSITY OF TRENTO - Italy



Scoring Exercise


- **CISCO host crash (CVE-2011-0355)**
 - Cisco Nexus 1000V Virtual Ethernet Module (VEM) 4.0(4) SV1(1) through SV1(3b), as used in VMware ESX 4.0 and 4.1 and ESXi 4.0 and 4.1, does not properly handle dropped packets, which allows guest OS users to cause a denial of service (ESX or ESXi host OS crash) by sending an 802.1Q tagged packet over an access vEthernet port, aka Cisco Bug ID CSCtj17451.

Attack Vector	A
Attack Complexity	L
Privileges Required	N
User Interaction	N
Scope	C
Confidentiality	N
Integrity	N
Availability	H


16/04/18

Fabio Massacci - CyberRisk Assessment

47



UNIVERSITY OF TRENTO - Italy



Scoring Exercise


- **Libvirt USB handling (CVE-2012-2693)**
 - libvirt, possibly before 0.9.12, does not properly assign USB devices to virtual machines when multiple devices have the same vendor and product ID, which might cause the wrong device to be associated with a guest and might allow local users to access unintended USB devices.

Attack Vector	L
Attack Complexity	H
Privileges Required	L
User Interaction	N
Scope	C
Confidentiality	L
Integrity	L
Availability	L


16/04/18

Fabio Massacci - CyberRisk Assessment

48



UNIVERSITY OF TRENTO - Italy



Scoring Exercise


- **SearchBlox Cross-Site Request Forgery Vulnerability (CVE-2015-0970)**
 - 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 Vector	N
Attack Complexity	L
Privileges Required	N
User Interaction	R
Scope	U
Confidentiality	H
Integrity	H
Availability	H


16/04/18

Fabio Massacci - CyberRisk Assessment

49



UNIVERSITY OF TRENTO - Italy



Scoring Exercise


- **phpMyAdmin Reflected Cross-site Scripting Vulnerability (CVE-2013-1937)**
 - 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 Vector	N
Attack Complexity	L
Privileges Required	N
User Interaction	R
Scope	C
Confidentiality	L
Integrity	L
Availability	N


16/04/18

Fabio Massacci - CyberRisk Assessment

50



UNIVERSITY
OF TRENTO - Italy



Scoring Exercise


- **Google Chrome Sandbox Bypass vulnerability (CVE-2012-5376)**
 - 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 Vector	N
Attack Complexity	L
Privileges Required	N
User Interaction	R
Scope	C
Confidentiality	H
Integrity	H
Availability	H


16/04/18

Fabio Massacci - CyberRisk Assessment

51



UNIVERSITY
OF TRENTO - Italy



Further reading

- **Chapters 10, 11 on Textbook**
- **Ross Anderson's book.**
- **CVSS First Web Site (See Wiki for links)**

16/04/18

Fabio Massacci - CyberRisk Assessment

52