AST

# Audit de Sécurité Technique

## Chapter 2.3
## Vulnerability Management

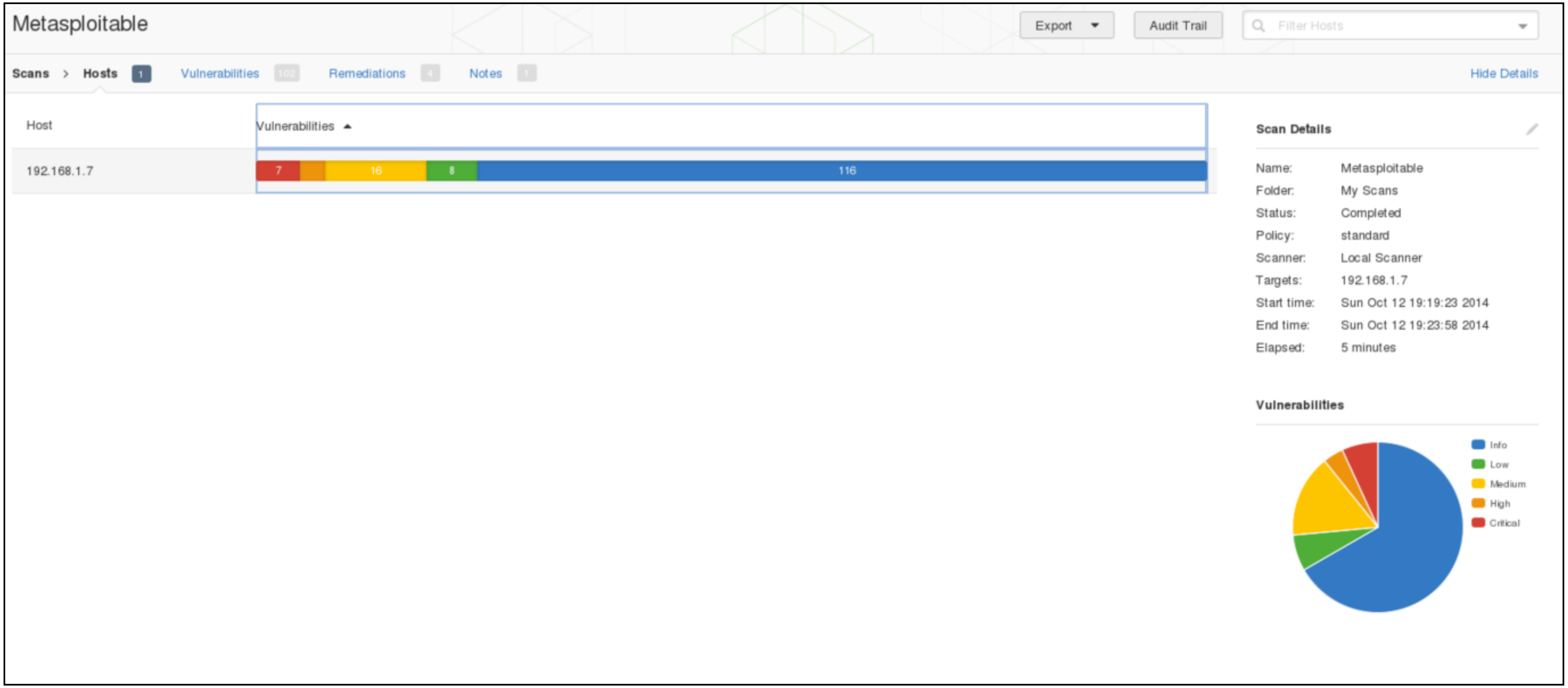
Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

# Information provided by the vulnerability scanner

- This is what you get when a nessus scan is completed



| Host | Vulnerabilities |
|---|---|
| 192.168.1.7 | 7 16 8 116 |

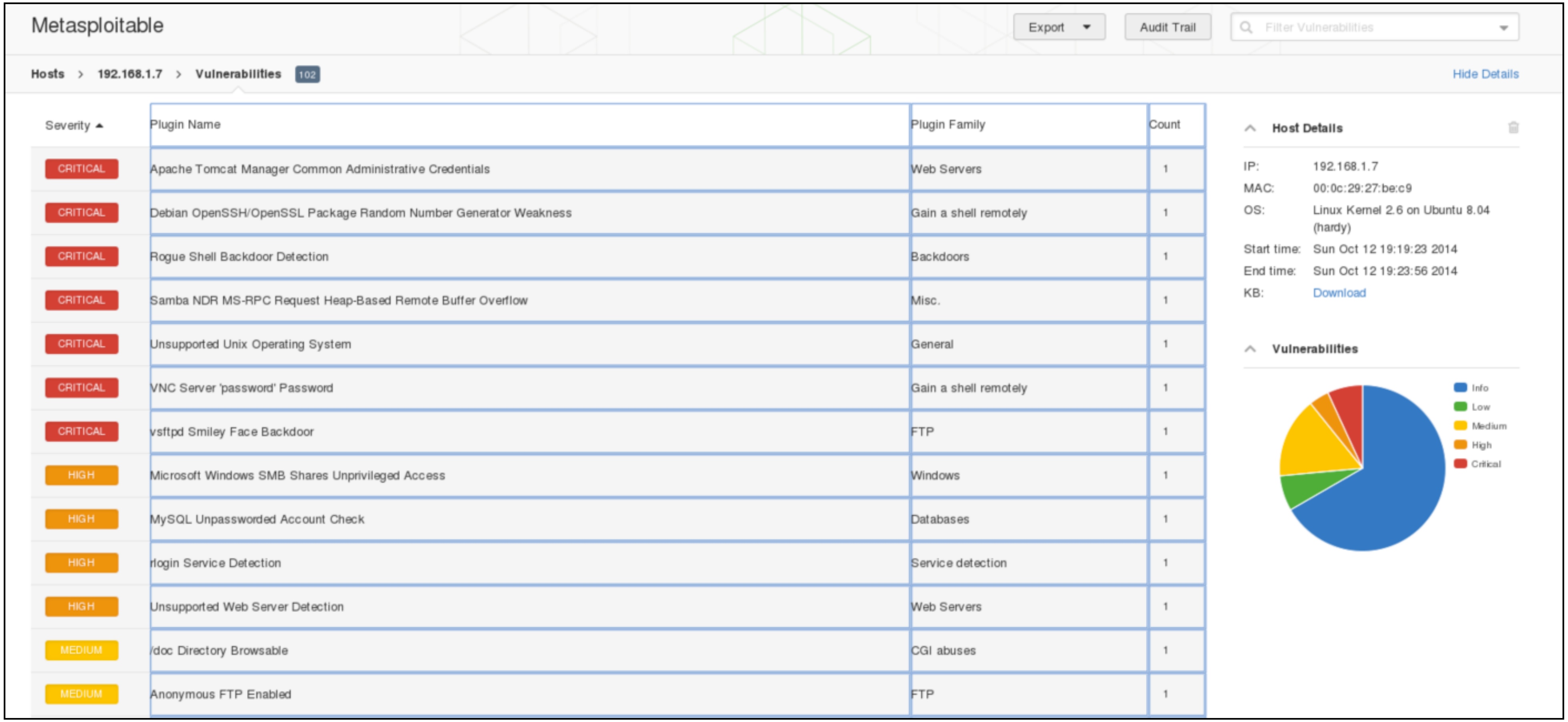
**Scan Details**

Name: Metasploitable
Folder: My Scans
Status: Completed
Policy: standard
Scanner: Local Scanner
Targets: 192.168.1.7
Start time: Sun Oct 12 19:19:23 2014
End time: Sun Oct 12 19:23:58 2014
Elapsed: 5 minutes

**Vulnerabilities**

# Information provided by the vulnerability scanner

- By clicking on the host you get a host information with vulnerability list, ordered by most critical ones



Metasploitable

Hosts > 192.168.1.7 > Vulnerabilities 102

| Severity ▲ | Plugin Name | Plugin Family | Count |
|---|---|---|---|
| CRITICAL | Apache Tomcat Manager Common Administrative Credentials | Web Servers | 1 |
| CRITICAL | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | Gain a shell remotely | 1 |
| CRITICAL | Rogue Shell Backdoor Detection | Backdoors | 1 |
| CRITICAL | Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow | Misc. | 1 |
| CRITICAL | Unsupported Unix Operating System | General | 1 |
| CRITICAL | VNC Server 'password' Password | Gain a shell remotely | 1 |
| CRITICAL | vsftpd Smiley Face Backdoor | FTP | 1 |
| HIGH | Microsoft Windows SMB Shares Unprivileged Access | Windows | 1 |
| HIGH | MySQL Unpassworded Account Check | Databases | 1 |
| HIGH | rlogin Service Detection | Service detection | 1 |
| HIGH | Unsupported Web Server Detection | Web Servers | 1 |
| MEDIUM | /doc Directory Browsable | CGI abuses | 1 |
| MEDIUM | Anonymous FTP Enabled | FTP | 1 |

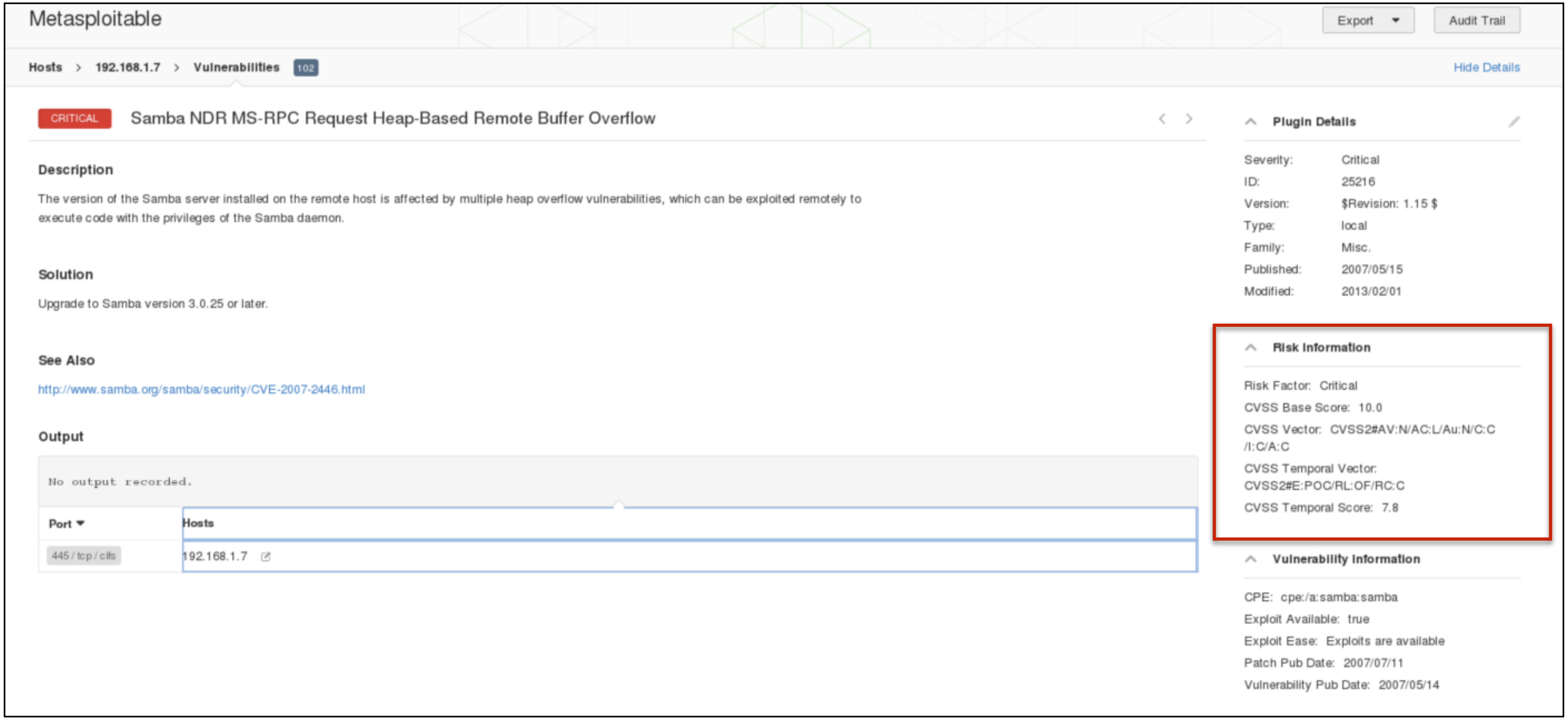
Host Details

| | |
|---|---|
| IP: | 192.168.1.7 |
| MAC: | 00:0c:29:27:be:c9 |
| OS: | Linux Kernel 2.6 on Ubuntu 8.04 (hardy) |
| Start time: | Sun Oct 12 19:19:23 2014 |
| End time: | Sun Oct 12 19:23:56 2014 |
| KB: | Download |

Vulnerabilities

# Information provided by the vulnerability scanner

- By clicking on the vulnerability, detailed information is shown



Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

**Description**

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

**Solution**

Upgrade to Samba version 3.0.25 or later.

**See Also**

http://www.samba.org/samba/security/CVE-2007-2446.html

**Output**

```
No output recorded.
```

| Port | Hosts |
|---|---|
| 445 / tcp / cifs | 192.168.1.7 |

**Plugin Details**

| | |
|---|---|
| Severity: | Critical |
| ID: | 25216 |
| Version: | $Revision: 1.15 $ |
| Type: | local |
| Family: | Misc. |
| Published: | 2007/05/15 |
| Modified: | 2013/02/01 |

**Risk Information**

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

CVSS Temporal Score: 7.8

**Vulnerability Information**

CPE: cpe:/a:samba:samba

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: 2007/07/11

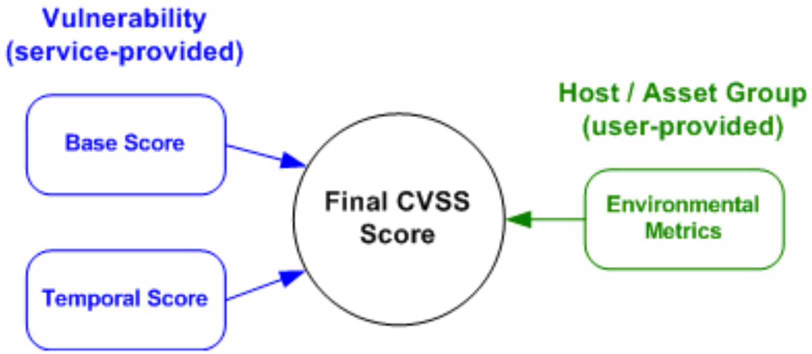
Vulnerability Pub Date: 2007/05/14

# Common Vulnerability Scoring System

- **Common Vulnerability Scoring System** (CVSS) - free and open industry convention for assessing the severity of computer system security vulnerabilities
- CVSS defines a vulnerability as a bug, flaw, weakness, or exposure of an application, system device, or service that could lead to a failure of confidentiality, integrity, or availability
- CVSS model attempts to ensure <u>repeatable</u> and <u>accurate</u> measurement while enabling users to view the underlying vulnerability characteristics used to generate <u>numerical scores</u>
- Two common uses of the CVSS are calculating the <u>severity</u> and <u>prioritization of vulnerability remediation activities</u>

# CVSS metrics structure

- CVSS score are calculated based on three metrics:
  - **Base Metrics** for qualities intrinsic to a vulnerability
  - **Temporal Metrics** for characteristics that evolve over the lifetime of vulnerability
  - **Environmental Metrics** for vulnerabilities that depend on a particular implementation or environment

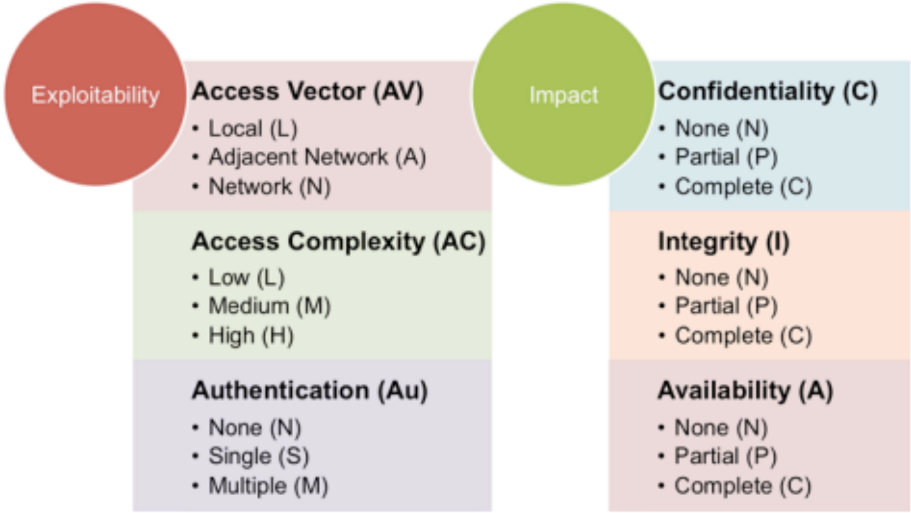


- These metrics generate a global score as well as a text vector indicating the severity of the vulnerability
  - Vectors are expressed via a machine-readable textual representation of the values used to derive the score.
  - The forward slash character ("/" ) is used to separate the metrics and square brackets are used to identify optional elements

*AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]*

# CVSS Base metrics

- **Exploitability**
  - The **access vector** (AV) shows how a vulnerability may be exploited.
  - The **access complexity** (AC) metric describes how easy or difficult it is to exploit the discovered vulnerability.
  - The **authentication** (Au) metric describes the number of times that an attacker must authenticate to a target to exploit it



Exploitability

**Access Vector (AV)**
- Local (L)
- Adjacent Network (A)
- Network (N)

**Access Complexity (AC)**
- Low (L)
- Medium (M)
- High (H)

**Authentication (Au)**
- None (N)
- Single (S)
- Multiple (M)

Impact

**Confidentiality (C)**
- None (N)
- Partial (P)
- Complete (C)

**Integrity (I)**
- None (N)
- Partial (P)
- Complete (C)

**Availability (A)**
- None (N)
- Partial (P)
- Complete (C)

- **Impact**
  - The **confidentiality** (C) metric describes the impact on the confidentiality of processed by the system
  - The **integrity** (I) metric describes the impact on the integrity of the exploited system.
  - The **availability** (A) metric describes the impact on the availability of the target system. Attacks that consume network bandwidth, processor cycles, memory or any other resources affect the availability of a system.

# Exploitability - Access Vector (AV)

| Value | Description | Score |
|---|---|---|
| **Local (L)** | The attacker must either have physical access to the vulnerable system (e.g. firewire attacks) or a local account (e.g. a privilege escalation attack). | **0.395** |
| **Adjacent Network (A)** | The attacker must have access to the broadcast or collision domain of the vulnerable system (e.g. ARP spoofing, bluetooth attacks). | **0.646** |
| **Network (N)** | The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service) | **1.0** |

# Exploitability - Access Complexity (AC)

| Value | Description | Score |
|---|---|---|
| **High (H)** | Specialised conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people. | **0.35** |
| **Medium (M)** | There are some additional requirements for access, such as a limit on the origin of the attacks, or a requirement for the vulnerable system to be running with an uncommon, non-default configuration. | **0.61** |
| **Low (L)** | There are no special conditions for access to the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous. | **0.71** |

# Exploitability - Authentication (Au)

| Value | Description | Score |
|---|---|---|
| **Multiple (M)** | Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. | **0.45** |
| **Single (S)** | The attacker must authenticate once in order to exploit the vulnerability. | **0.56** |
| **None (N)** | There is no requirement for the attacker to authenticate. | **0.704** |

For locally exploitable vulnerabilities, the **Au** should only be set to Single or Multiple if further authentication is required after initial access

# Impact - Confidentiality (C) and Integrity (I)

| Value | Confidentiality<br>Description | Score |
|---|---|---|
| **None (N)** | There is no impact on the confidentiality of the system. | **0** |
| **Partial (P)** | There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available. | **0.275** |
| **Complete (C)** | There is total information disclosure, providing access to any / all data on the system. | **0.66** |

| Value | Integrity<br>Description | Score |
|---|---|---|
| **None (N)** | There is no impact on the integrity of the system. | **0** |
| **Partial (P)** | Modification of some data or system files is possible, but the scope of the modification is limited. | **0.275** |
| **Complete (C)** | There is total loss of integrity; the attacker can modify any files or information on the target system. | **0.66** |

# Impact - Availability (A)

| | Availability | |
|---|---|---|
| **Value** | **Description** | **Score** |
| **None (N)** | There is no impact on the integrity of the system. | **0** |
| **Partial (P)** | There is reduced performance or loss of some functionality. | **0.275** |
| **Complete (C)** | There is total loss of availability of the attacked resource. | **0.66** |

# Calculating the CVSS Base score

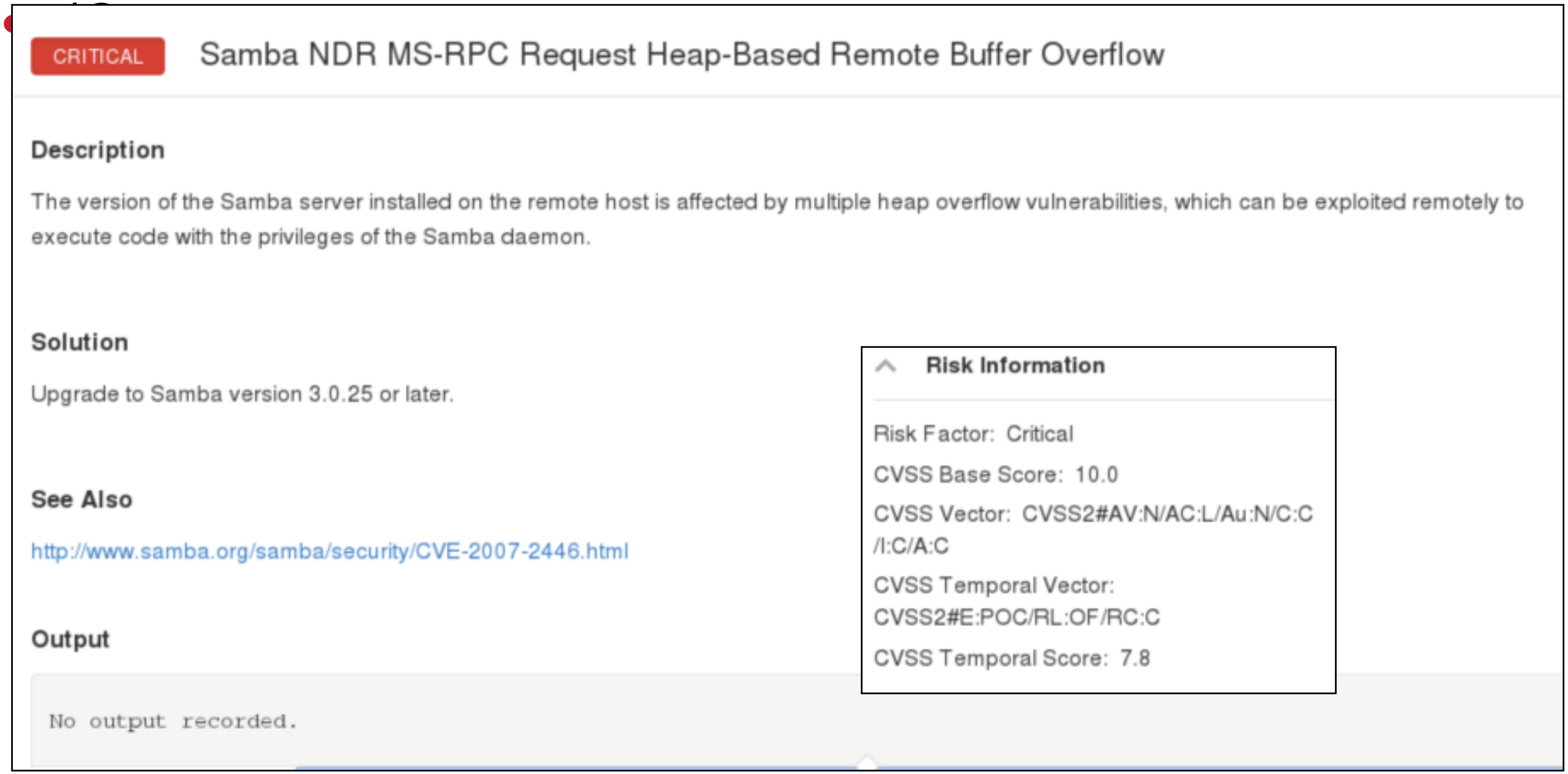
$$Exploitability = 20 \times AV \times AC \times Au$$

$$Impact = 10.41 \times (1 - (1 - C) \times (1 - I) \times (1 - A))$$

$$\boxed{Base\ Score = ((0.6 \times Impact) + (0.4 \times Exploitability) - 1.5) \times f(Impact)}$$

$$where\ f(Impact) = 0\ if\ Impact = 0,\ \text{and } 1.176 \text{ otherwise}$$

# Example - back to Nessus



CRITICAL Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

**Description**

The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

**Solution**

Upgrade to Samba version 3.0.25 or later.

**See Also**

http://www.samba.org/samba/security/CVE-2007-2446.html

**Output**

```
No output recorded.
```

**Risk Information**

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

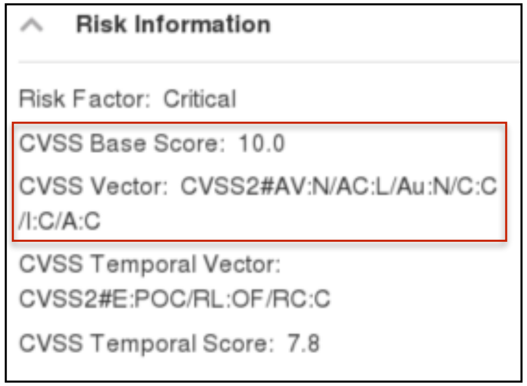
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

CVSS Temporal Score: 7.8

# Example - Calculating CVSS Base score

| | Exploitability | |
|---|---|---|
| Parameter | Value | Score |
| **Access Vector (AV)** | Network (N) - Remotely exploitable | **1** |
| **Access Complexity (AC)** | Low (L) - No special condition is required | **0.71** |
| **Authentication** | None (N) - No requirement for the attacker to authenticate | **0.704** |

| | Impact | |
|---|---|---|
| Parameter | Value | Score |
| **Confidentiality (C)** | Complete (C) - Total information disclosure | **0.66** |
| **Integrity (I)** | Complete (C) - Total loss of integrity | **0.66** |
| **Availability (A)** | Complete (C) - Total loss of availability | **0.66** |



**Risk Information**

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

CVSS Temporal Score: 7.8

$$Exploitability = 20 \times 1 \times 0.71 \times 0.704 = 10$$

$$Impact = 10.41 \times (1 - (1 - 0.66) \times (1 - 0.66) \times (1 - 0.66) = 10$$

$$Base\ Score = ((0.6 \times 10) + (0.4 \times 10) - 1.5) * 1.176 = 10$$

# CVSS Temporal Metrics

- The Temporal Metric group reflects the evolution over the lifetime of the vulnerability
  - Exploits are developed, disclosed and automated
  - Patches and fixes are made available
- 3 metrics to describe this evolution
  - **Exploitability** (E) metric describes the current state of exploitation techniques or automated exploitation code.
  - **Remediation level** (RL) of a vulnerability allows the temporal score of a vulnerability to decrease as mitigations and official fixes are made available.
  - **Report confidence** (RC) of a vulnerability measures the level of confidence in the existence of the vulnerability and also the credibility of the technical details of the vulnerability.

# Temporal - Exploitability (E)

| Value | Description | Score |
|---|---|---|
| **Unproven (U)** | No exploit code is available, or the exploit is theoretical | **0.85** |
| **Proof-of-Concept (P)** | Proof-of-concept exploit code or demonstration attacks are available, but not practical for widespread use. Not functional against all instances of the vulnerability. | **0.9** |
| **Functional (F)** | Functional exploit code is available, and works in most situations where the vulnerability is present. | **0.95** |
| **High (H)** | The vulnerability can be exploited by automated code, including mobile code (such as a worm or virus). | **1** |
| **Not Defined (ND)** | This is a signal to ignore this score. | **ND** |

# Temporal - Remediation Level (RL)

| Value | Description | Score |
|---|---|---|
| Official Fix (O) | A complete vendor solution is available - either a patch or an upgrade. | 0.87 |
| Temporary Fix (T) | There is an official but temporary fix / mitigation available from the vendor. | 0.9 |
| Workaround (W) | There is an unofficial, non-vendor solution or mitigation available - perhaps developed or suggested by users of the affected product or another third party. | 0.95 |
| Unavailable (U) | There is no solution available, or it is impossible to apply a suggested solution. This is the usual initial state of the remediation level when a vulnerability is identified. | 1 |
| Not Defined (ND) | This is a signal to ignore this score. | ND |

# Temporal - Report Confidence (RC)

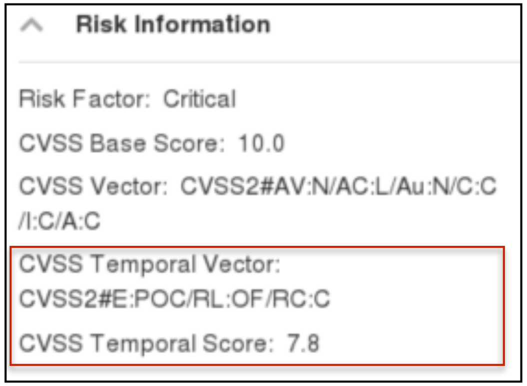
| Value | Description | Score |
|---|---|---|
| **Unconfirmed (UC)** | A single unconfirmed source, or multiple conflicting sources. Rumored vulnerability. | **0.9** |
| **Uncorroborated (UR)** | Multiple sources that broadly agree - there may be a level of remaining uncertainty about the vulnerability | **0.95** |
| **Confirmed (C)** | Acknowledged and confirmed by the vendor or manufacturer of the affected product. | **1** |
| **Not Defined (ND)** | This is a signal to ignore this score. | **ND** |

# Calculating the CVSS Temporal score

$$\boxed{Temporal\ Score = Base\ Score \times E \times RL \times RC}$$

- Example

| | Temporal | |
|---|---|---|
| **Parameter** | **Value** | **Score** |
| **Exploitability (E)** | (P) Proof-of-concept exploit code or demonstration attacks are available | **0.9** |
| **Remediation Level (RL)** | (O) Official solution exists | **0.87** |
| **Report Confidence (RC)** | (C) Confirmed by the vendor/manufacturer | **1** |



**Risk Information**

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

CVSS Temporal Score: 7.8

$$\boxed{Temporal\ Score = 10 \times 0.9 \times 0.87 \times 1 = 7.8}$$

# CVSS Environmental Metrics

- Environmental Metrics help to project the score on the specific context of the given organisation
- This score is calculated subjectively by the concerned organisation (people who know the context)
- 5 metrics:
  - **Collateral damage potential** (CDP) metric measures the potential loss or impact on either physical assets such as equipment (and lives), or the financial impact upon the affected organisation if the vulnerability is exploited
  - **Target distribution** (TD) metric measures the proportion of vulnerable systems in the environment
  - Three metrics assess the **specific security** requirements for **confidentiality** (CR), **integrity** (IR) and **availability** (AR), allowing the environmental score to be fine-tuned according to the customer's environment.

# Environmental - Collateral Damage Potential (CDP)

| Value | Description | Score |
|---|---|---|
| **None (N)** | No potential for loss of property, revenue or productivity | **0** |
| **Low (L)** | Slight damage to assets, or minor loss of revenue or productivity | **0.1** |
| **Low-Medium (LM)** | Moderate damage or loss | **0.3** |
| **Medium-High (MH)** | Significant damage or loss | **0.4** |
| **High (H)** | Catastrophic damage or loss | **0.5** |
| **Not Defined (ND)** | This is a signal to ignore this score. | **ND** |

# Environmental - Target Distribution (TD)

| Value | Description | Score |
|---|---|---|
| None (N) | No target systems exist, or they only exist in laboratory settings | 0 |
| Low (L) | 1%-25% of systems at risk | 0.25 |
| Medium (M) | 26%-75% of systems at risk | 0.75 |
| High (H) | 76%-100% of systems at risk | 1.0 |
| Not Defined (ND) | This is a signal to ignore this score. | ND |

# Environmental - Security Requirements Confidentiality (CR), Integrity (IR), Availability (AR)

| Value | Description | Score |
|---|---|---|
| **Low (L)** | Loss of (confidentiality / integrity / availability) is likely to have only a limited effect on the organisation. | **0.5** |
| **Medium (M)** | Loss of (confidentiality / integrity / availability) is likely to have a serious effect on the organisation. | **1.0** |
| **High (H)** | Loss of (confidentiality / integrity / availability) is likely to have a catastrophic effect on the organisation. | **1.51** |
| **Not Defined (ND)** | This is a signal to ignore this score. | **1.0** |

# Environmental Score Calculation

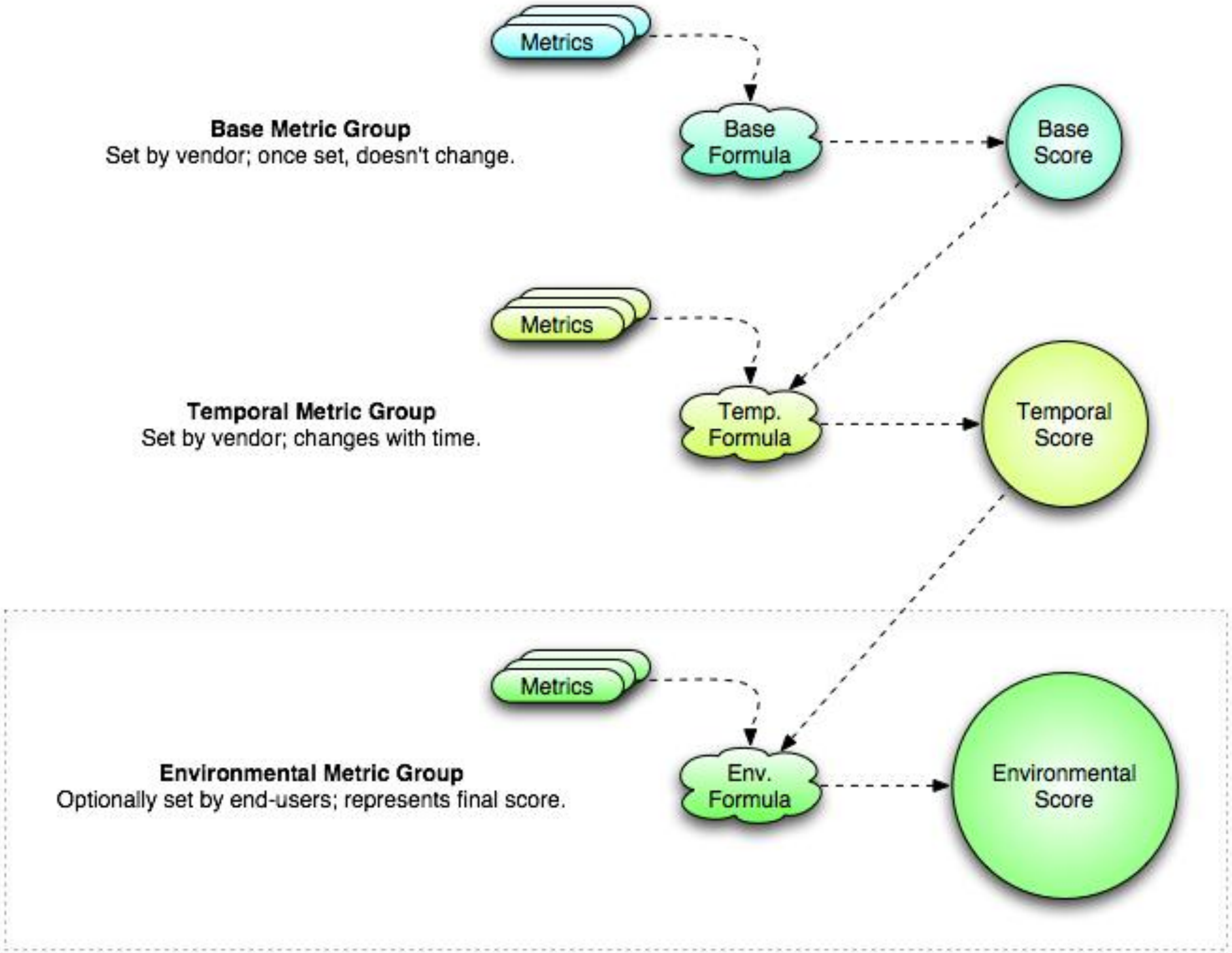
- Final score taking into account all subscores is calculated as

$$Adjusted\ Impact = min(10, 10.41 \times (1 - (1 - C \times CR) \times (1 - I \times IR) \times (1 - A \times AR)))$$

$$Adjusted\ Temporal = Adjusted\ Impact \times E \times RL \times RC$$

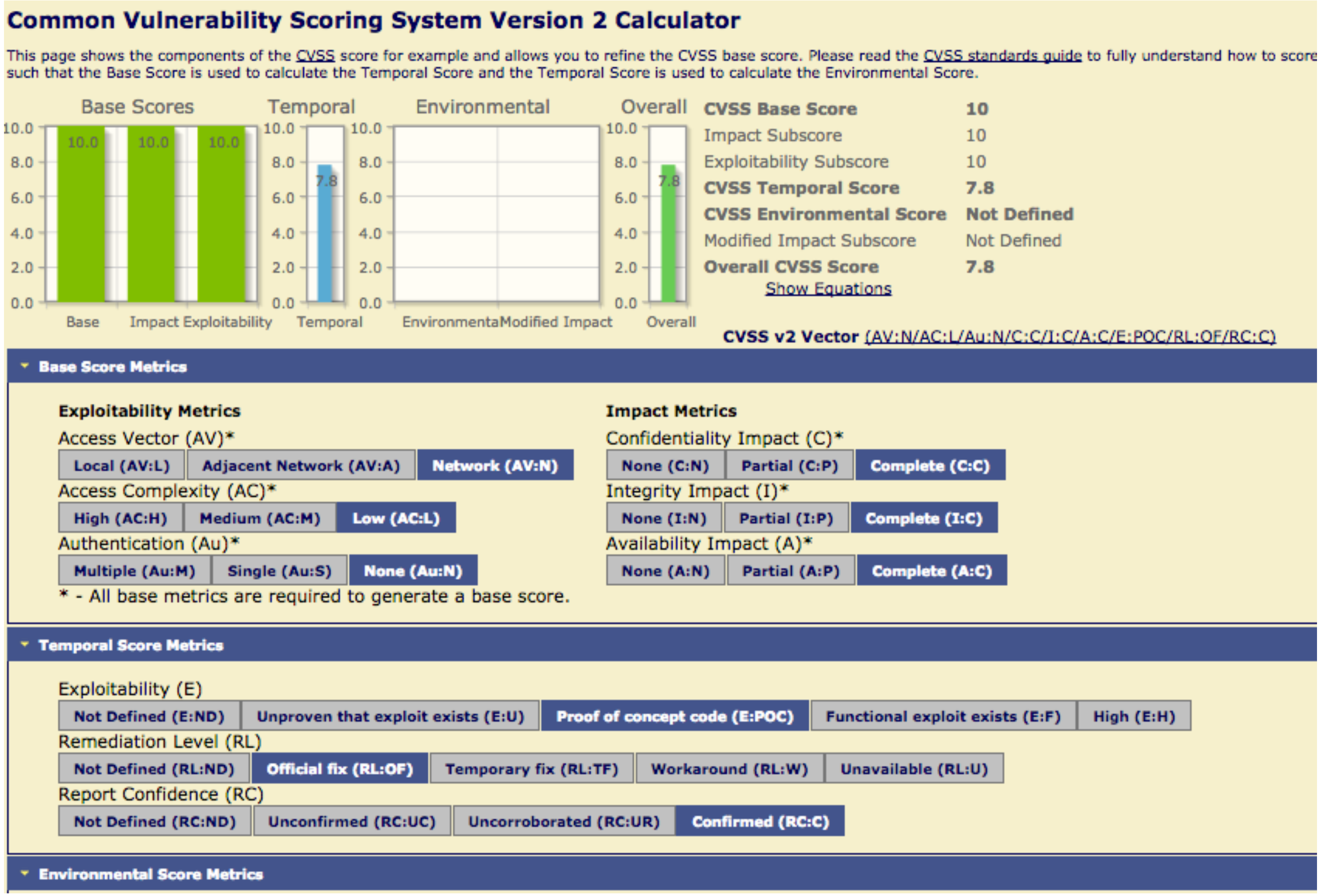
$$\boxed{Environmental\ Score = (Adjusted\ Temporal + (10 - Adjusted\ Temporal) \times CDP) \times TD}$$

# CVSS Global Formula



Metrics
Base Metric Group
Set by vendor; once set, doesn't change.
Base Formula
Base Score
Metrics
Temporal Metric Group
Set by vendor; changes with time.
Temp. Formula
Temporal Score
Metrics
Environmental Metric Group
Optionally set by end-users; represents final score.
Env. Formula
Environmental Score

# CVSS Calculator



## Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

| | |
|---|---|
| **CVSS Base Score** | **10** |
| Impact Subscore | 10 |
| Exploitability Subscore | 10 |
| **CVSS Temporal Score** | **7.8** |
| **CVSS Environmental Score** | **Not Defined** |
| Modified Impact Subscore | Not Defined |
| **Overall CVSS Score** | **7.8** |

Show Equations

**CVSS v2 Vector** (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)

**Base Score Metrics**

**Exploitability Metrics**

Access Vector (AV)*

Local (AV:L) | Adjacent Network (AV:A) | [✓ Network (AV:N)]

Access Complexity (AC)*

High (AC:H) | Medium (AC:M) | [✓ Low (AC:L)]

Authentication (Au)*

Multiple (Au:M) | Single (Au:S) | [✓ None (Au:N)]

* - All base metrics are required to generate a base score.

**Impact Metrics**

Confidentiality Impact (C)*

None (C:N) | Partial (C:P) | [✓ Complete (C:C)]

Integrity Impact (I)*

None (I:N) | Partial (I:P) | [✓ Complete (I:C)]

Availability Impact (A)*

None (A:N) | Partial (A:P) | [✓ Complete (A:C)]

**Temporal Score Metrics**

Exploitability (E)

Not Defined (E:ND) | Unproven that exploit exists (E:U) | [✓ Proof of concept code (E:POC)] | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:ND) | [✓ Official fix (RL:OF)] | Temporary fix (RL:TF) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) | Unconfirmed (RC:UC) | Uncorroborated (RC:UR) | [✓ Confirmed (RC:C)]

**Environmental Score Metrics**

http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2#score

# Limitations of CVSS system

- The CVSS specification is meant to score the impact to the system containing the vulnerability, not any downstream impact to other systems
- The CVSS base score discounts the impact of a vulnerability, is when that vulnerability is discovered within a protocol
  - example: Kaminsky bug
  - Environmental metrics provide some remedy
- Reliance solely on CVSS base metrics without accounting for temporal aspects and/or environmental specific circumstances of a vulnerability may lead to organizations improperly measuring the severity of a vulnerability
- Vulnerability assessment via the CVSS can assist in conducting risk assessments, **but the CVSS scores should not be the sole factor when determining risk**
- CVSS score represents the impact of an individual vulnerability residing within an information system, and **does not account for vulnerability chaining**