

CVSS v4.0: Beyond the Numbers

Nick Leali, FIRST CVSS SIG Co-Chair
March 25, 2024

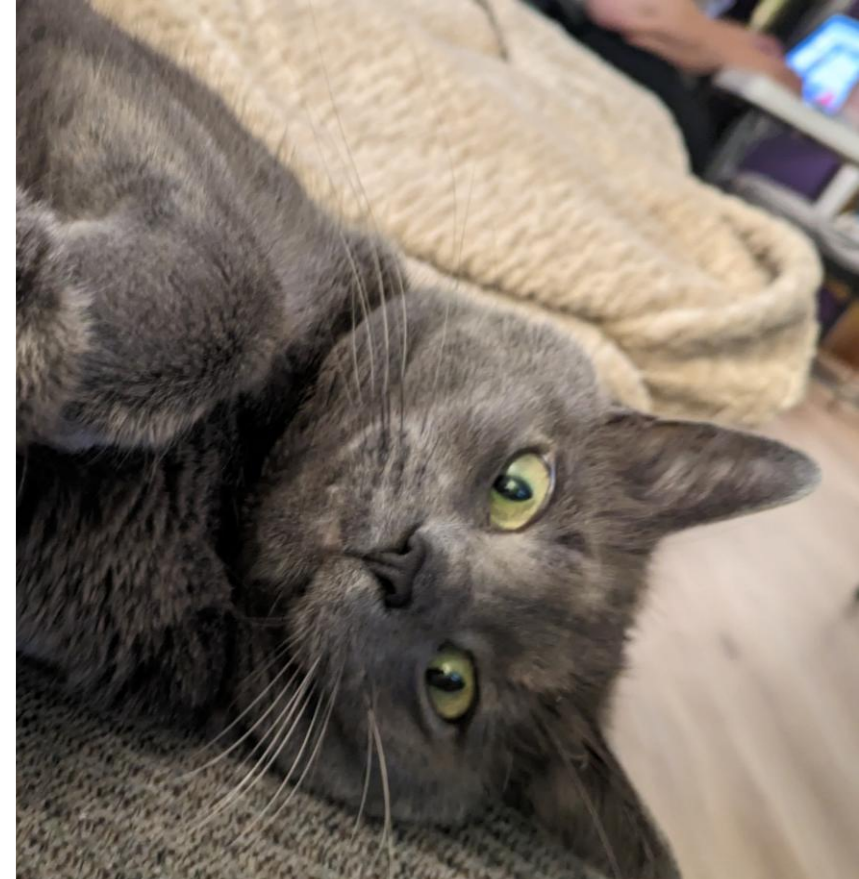
Agenda

- 1 Introduction
- 2 The Base Score Problem
- 3 What's New With CVSS v4.0
- 4 Useful New Metrics
- 5 Case Study / Demo
- 6 Resources



Chairs

- Dale Rich
- Nick Leali



whoami – Nick Leali

Why I'm
here:

*“Everything
Is a 9.8”*

Inspired by ICS / OT CVSS Examples

Check out CVE-2022-47379

How to better distinguish scores

Discuss the use of tuned CVSS

Threat with KEV lookup

Supplemental Metrics

Environmental Metrics

End goal: separate the wheat from the chaff

The Base Score Fidelity Problem

CVSS is not just the base score

- This is not new with CVSS v4.0

Vendors provide a base score

- The base score only goes so far

How can we provide more details?

- CVSS v4.0 provides more tools

Why Do We See Only Base Scores

Difficult and Complex

- We can't know customers environments
- Time to investigate
- Legal and compliance concerns

Business Opportunity

- Or it's offloaded to other processes and services

Lack of Demand

- Many organizations are not mature enough

What is new with



v4.0?

New CVSS Features

- Finer granularity, new Base metrics
- New Base metric: Attack Requirements (AT)
- New Base metric values: User Interaction (UI): Passive (P) and Active (A)
- Temporal renamed to Threat
- Metrics simplified and clarified
- Remediation Level (RL) and Report Confidence (RC) retired
- Exploit "Code" Maturity renamed to Exploit Maturity (E) with clearer values



CVSS v4.0 Score Nomenclature

The CVSS Standard is NOT just the Base Score

To stress this concept, new nomenclature has been adopted:

- CVSS-B: CVSS Base Score
- CVSS-BT: CVSS Base + Threat Score
- CVSS-BE: CVSS Base + Environmental Score
- CVSS-BTE: CVSS Base + Threat + Environmental Score

The more metrics used to enrich your CVSS scoring, the higher quality your assessment will be.

Distinguishing Features: Base Metrics

Focus on: User Interaction

Passive: ...*limited interaction by the targeted user with the vulnerable system and the attacker's payload...*

Active: ...*perform specific, conscious interactions with the vulnerable system and the attacker's payload...*

Two XSS examples, Stored vs. Reflected

CVE-2020-0926: A user must browse within a web application

CVE-2022-24682: A user must click a link

	Numeric Score	Vector String
CVE-2020-0926	(v4.0 Base) 5.1	CVSS:4.0/AV:N/AC:L/AT:N/ PR:L/UI:P /VC:N/VI:L/VA:N/SC:L/SI:L/SA:N
CVE-2022-24682	(v4.0 Base) 5.1	CVSS:4.0/AV:N/AC:L/AT:N/ PR:N/UI:A /VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

Focus on: Attack Requirements

Attack Requirements: ...the prerequisite deployment and execution conditions or variables of the vulnerable system that enable the attack...

The metric is related to external challenges: Deployment and execution conditions or variables of the vulnerable system must be overcome. Examples include: race condition or network injection (MITM).

CVE-2020-3549: Cisco FMC and FTD Hash Theft

An attacker must be able to observe traffic between hosts, an on-path attack.

Numeric Score	Vector String
(v4.0 Base) 9.2	CVSS:4.0/AV:N/AC:L/ AT:P /PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Focus on: Subsequent System Impact

Subsequent System Confidentiality, Integrity, and Availability: ...*assessment providers need to account for impacts both to the Vulnerable System and impacts outside of the Vulnerable System...*

CVE-2023-22394: Junos OS Memory Leak DoS

Subsequent systems, i.e. other hosts using the vulnerable device as a gateway, are impacted, and the SA:L metric is selected.

Numeric Score	Vector String
(v4.0 Base) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
(v4.0 B+T) 6.6	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/E:U

Additional Subsequent System Impact Example

Subsequent System Confidentiality, Integrity, and Availability: ...*assessment providers need to account for impacts both to the Vulnerable System and impacts outside of the Vulnerable System...*

CVE-2020-3947: VMware Use-After-Free

A user within the guest operating system could execute arbitrary code on the host. A successful exploit could allow the attacker to impact the host and other virtual machines as a result.

Numeric Score	Vector String
(v4.0 Base) 9.4	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
(v4.0 Base) 8.6	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Threat Metrics

Time for a change

Threat Metrics in CVSS v4.0

Removed Remediation Level

Removed Report Confidence

Threat Metrics in Detail

- Unreported
- POC
- Attacked
- Not Defined

Environmental Metrics

Making CVSS Personal

Brief Environmental Overview

Modified Base Metrics

- Allows end user to adapt scores
- A few accepted best practices
- Allows much more relevant impacts

Environmental Security Requirements

- Changes score rating per impact metric
- Puts greater emphasis on organizational requirements

Context Clues: Supplemental Metrics

What are Supplemental Metrics

Qualitative attribute of the
vulnerability

Does not change the
numeric score

Allows consumers to
distinguish non-impact
qualities

Focus on: Safety

Safety: ...indicates the degree of impact to the Safety of a human actor or participant that can be predictably injured as a result of the vulnerability being exploited...

CVE-2023-28728: Panasonic Control FPWIN ICS Buffer Overflow

The impact from an attacker gaining full control of software that is running on a programmable logic controller (PLC) may meet the definition of IEC 61508 consequence category marginal, critical or catastrophic.

Numeric Score	Vector String
(v4.0 Base) 8.5	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
(v4.0 Base+S) 8.5	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:P

Focus on: Automatable

Automatable: Can an attacker automate exploitation events for this vulnerability across multiple targets?

CVE-2099-10002: 2099-01 Security Bulletin: Junos: RPD core due to processing and forwarding of BGP UPDATE with malformed optional transitive attributes

A BGP UPDATE containing a specifically crafted set of transitive attributes can cause the RPD routing process to crash and restart. The RPD process forwards the BGP UPDATE, then crashes and restarts, resulting in a cascade Denial of Service (DoS) of the router, and all downstream routers.

Numeric Score	Vector String
(v4.0 Base) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
(v4.0 Base+S) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/AU:Y/U:Red

Focus on: Provider Urgency

To facilitate a standardized method to incorporate additional provider-supplied assessment, an optional “pass-through” Supplemental Metric called Provider Urgency is available.

CVE-2099-10001: 2099-01 Security Bulletin: Junos: RPD core due to receipt of BGP UPDATE with malformed optional transitive attributes

A BGP UPDATE containing a specifically crafted set of transitive attributes can cause the RPD routing process to crash and restart. The RPD process crashes immediately upon receipt of the BGP UPDATE, resulting in a Denial of Service (DoS) of the router.

Numeric Score	Vector String
(v4.0 Base) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
(v4.0 Base+S) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L/AU:N/U:Amber

Focus on: Recovery

Recovery: ...describes the resilience of a system to recover services, in terms of performance and availability, after an attack has been performed...

CVE-2016-5729: Lenovo Thinkpwn Exploit

The attacker could ... prevent recovery of the system ... and locking down the system.

Numeric Score	Vector String
(v4.0 Base) 9.3	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
(v4.0 Base+S) 9.3	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/R:I

Focus on: Value Density

Value Density: ...*describes the resources that the attacker will gain control over with a single exploitation event...*

CVE-2022-26923: Active Directory Privilege Escalation

An authenticated user could manipulate attributes on computer accounts they own or manage, and acquire a certificate from Active Directory Certificate Services that would allow elevation of privilege to System.

Numeric Score	Vector String
(v4.0 Base) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
(v4.0 Base+S) 8.7	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/V:C

Focus on: Vulnerability Response Effort

Vulnerability Response Effort: *...how difficult it is for consumers to provide an initial response to the impact of vulnerabilities for deployed products and services in their infrastructure...*

CVE-2019-1834: Cisco Aironet Denial of Service

Administrators can configure the switch interface ... to drop any new learned MAC addresses.

Numeric Score	Vector String
(v4.0 Base) 7.1	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
(v4.0 Base+S) 7.1	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/RE:L

Enriching the CVSS Base Score

Score Modification Methodology

Threat / CISA Check

- User Guide 3.2

AV:N -> MAV:A

- User Guide 3.8

Impact modification

- What devices are in my environment

The Best of CVEs, the Worst of CVEs

Heartbleed

CVE-2014-0160

Present in CISA KEV

AV:Network, uncontrolled

CVSS v4.0 Base 8.7

ClamAV Buffer Overflow


CVE-2023-20032

Not present in CISA KEV

AV:Network, controlled

CVSS v4.0 Base 9.3

CVSS v4.0 Base Scores



8.7

CVE-2014-0160

“Heartbleed”



9.3

CVE-2023-20032

ClamAV

CVSS v4.0 Base + Threat Scores

Added
E:A

8.7


CVE-2014-0160
“Heartbleed”

Added
E:U

8.1

CVE-2023-20032
ClamAV

CVSS v4.0 B+T+E Scores



8.7

CVE-2014-0160

“Heartbleed”




6.3

CVE-2023-20032

ClamAV

Added
MAV:A


CVSS v4.0 B+T+E Scores, Alternate



8.7

CVE-2014-0160

“Heartbleed”



2.7

CVE-2023-20032

ClamAV

Added
MVC:N
MVI:N
MVA:L

The Story of 2.7

01

CVE does not
appear in CISA
KEV

02

AV still
Network

03

No
confidentiality
or integrity
impact

04

Reduced
availability
impact

Tooling

Simple example for automation

Simple code: mycvss

API and CLI

Uses cvss4py library for math

Can be scripted

Use in front or alongside of feeds

CVSS v4.0 metric string:

CVE:

Evaluate my CVE.

Your base score is:

9.3

Your modified CVSS score is:

6.3

Lessons Learned

More than a base score

Takeaways

CVSS base scores are basic

Enrich those scores through several means

Help provide customers the path to improve for themselves

Questions?

Thank You!

Additional Resources

- CVSS v4.0 Training
 - https://learn.first.org/catalog/info/id:126,cms_featured_course:1
- CVSS Feedback
 - cvss@first.org
- CVSS Tooling
 - <https://github.com/FIRSTdotorg/cvss-v4-calculator>
 - <https://github.com/nickleali/mycvss>
- Join CVSS SIG
 - <https://portal.first.org/g/CVSS%20SIG/join>

CVSS v4.0 Site

<https://www.first.org/cvss/v4/>

- CVSS Documents
 - <https://www.first.org/cvss/v4.0/specification-document>
 - <https://www.first.org/cvss/calculator/4.0>
 - <https://www.first.org/cvss/v4.0/user-guide>
 - <https://www.first.org/cvss/v4.0/examples>