

CVSS IV THE VOYAGE HOME

Presented to Queen City Conference 0x1

Justin Hall, Sr Research Manager, Tenable



```
$ finger @localhost
```

```
Login: jhall
```

```
Name: Justin Hall
```

```
Directory: /home/jhall
```

```
Shell: /bin/bash
```

```
No mail.
```

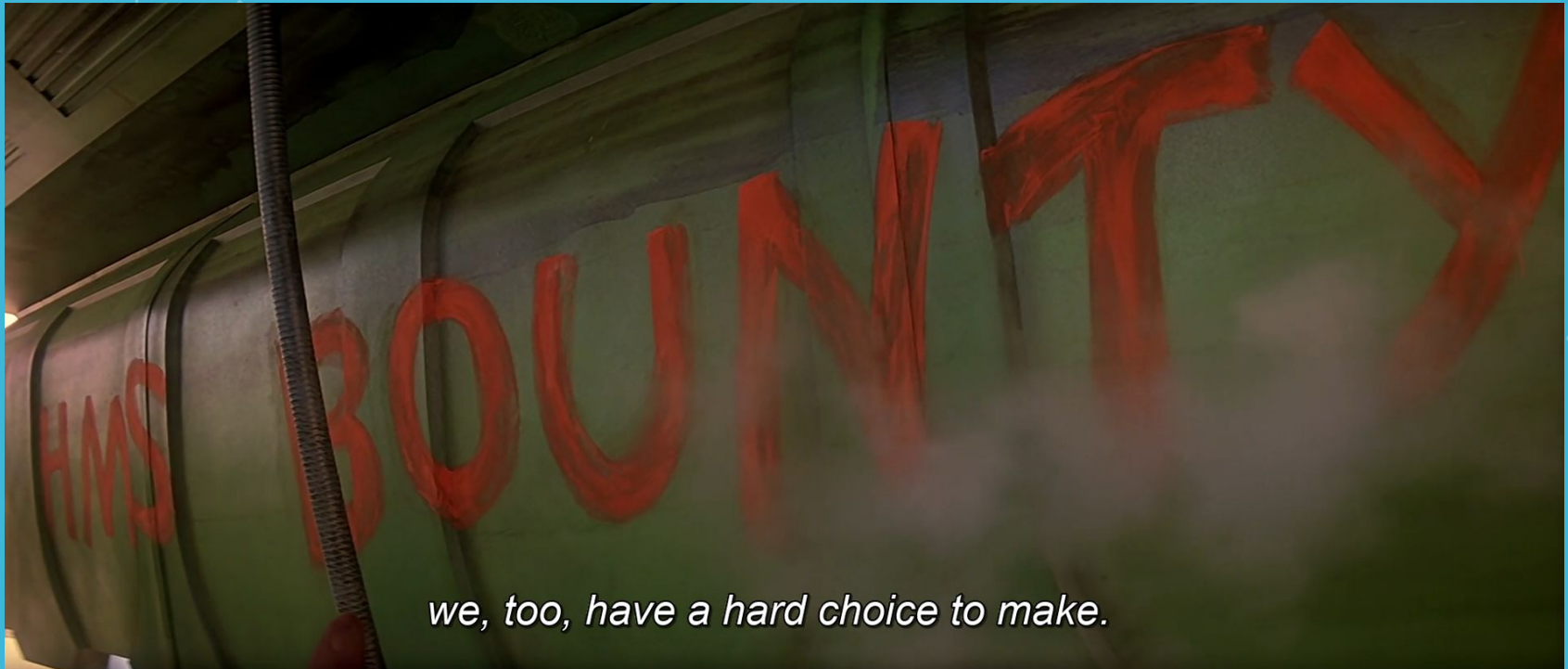
```
Sr Manager, Research @ Tenable
```

```
27 years in IT
```

```
18 years in infosec
```

```
Husband, dad, Jesus follower, nerd
```

Consider two vulnerabilities:



we, too, have a hard choice to make.

Consider two vulnerabilities:

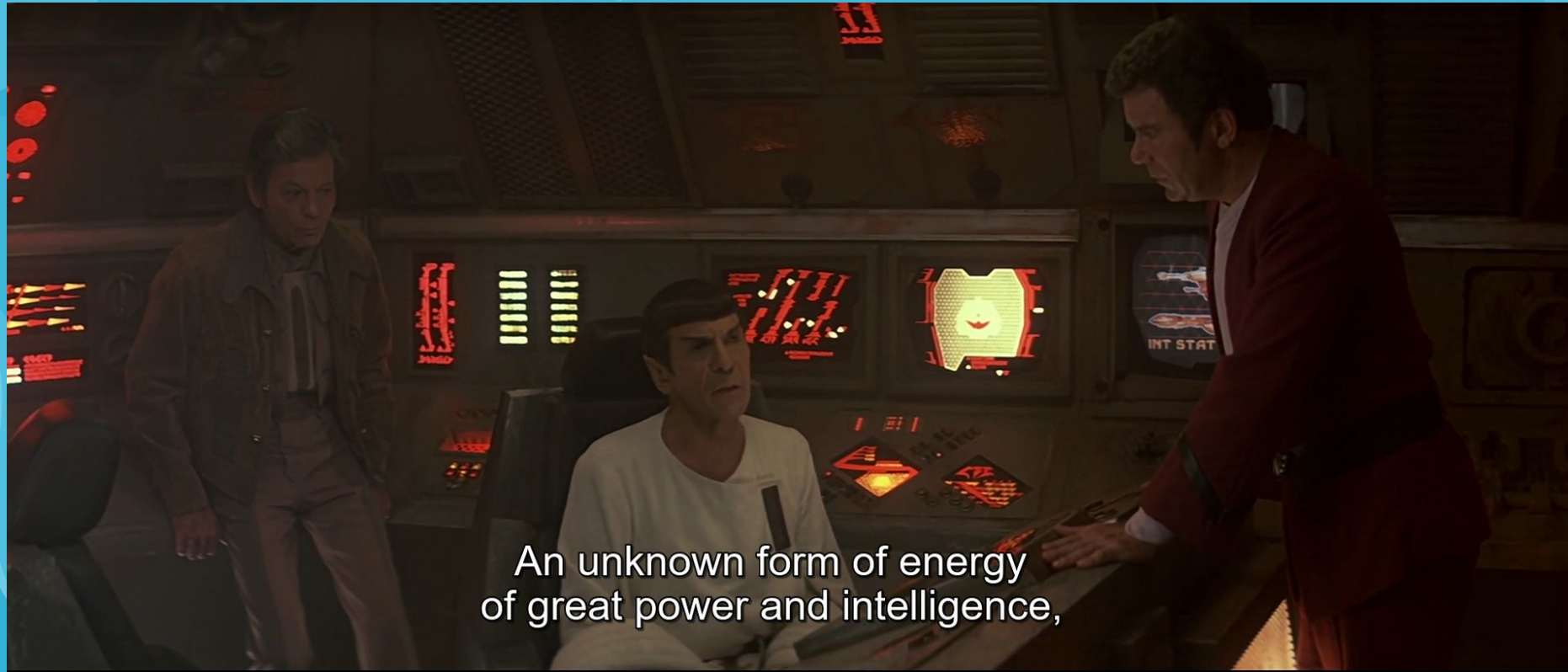
CVE-2023-21746

Local privilege
escalation
vulnerability in
Windows

CVE-2023-20198

Remote privilege
escalation
vulnerability on
Cisco IOS XE

What is CVSS?



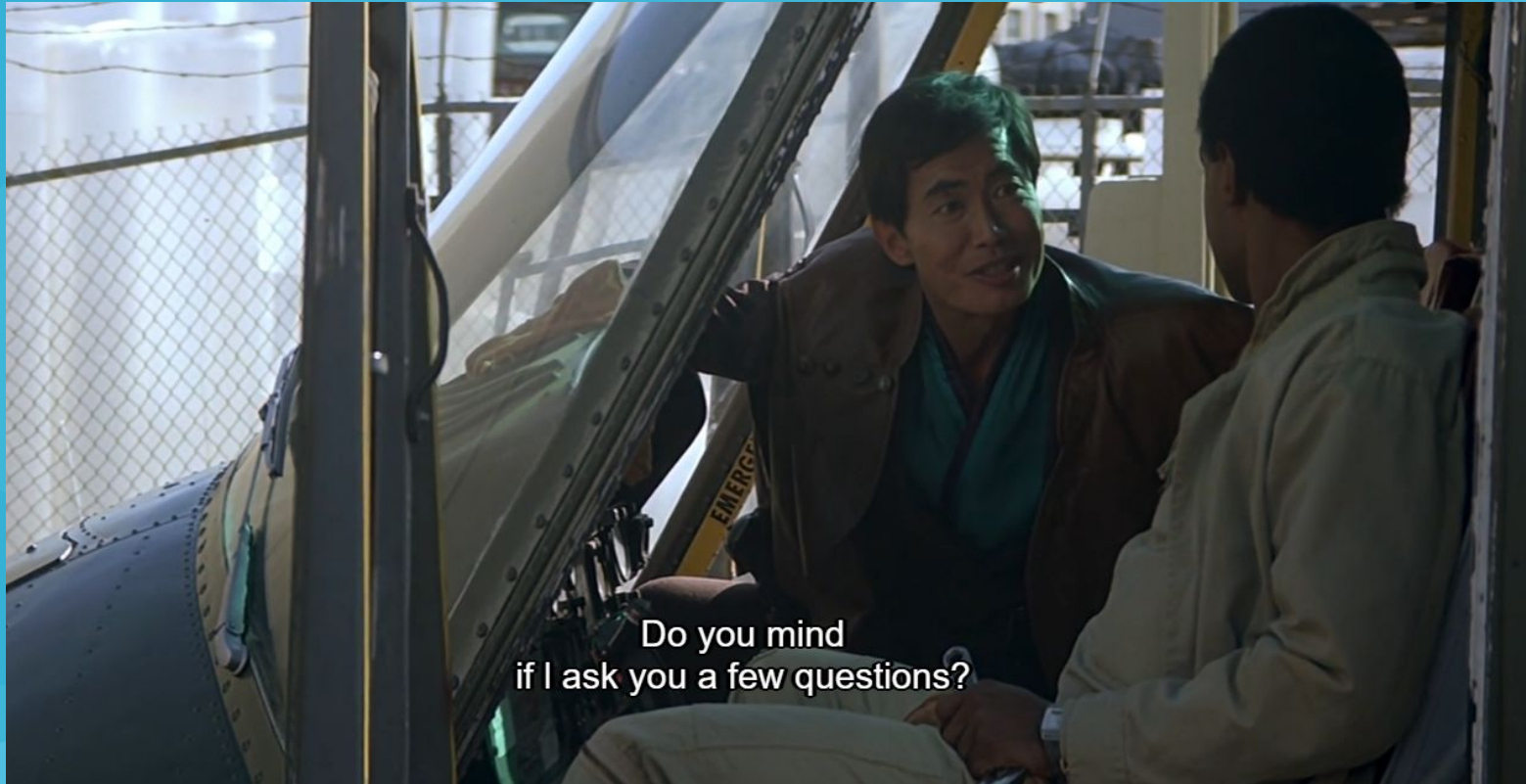
An unknown form of energy
of great power and intelligence,

What is CVSS?

“The Common Vulnerability Scoring System provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.”

FIRST, maintainers of CVSS

Poll Time!



A quick primer on using CVSS



A Quick Primer on CVSS

Let's score CVE-2023-21746

FIRST CVSSv4 Calculator

Vendor Bulletin

A Quick Primer on CVSS

Let's score CVE-2023-21746

Base Score: 8.5 (High)

Vector String:

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Updates in CVSSv4



*Thanks, Will Christman

Changes to Base metrics



Excuse me, sir, can you direct me to the naval base in Alameda?

Changes to Base metrics

Attack Requirements

Base Metrics ?

Exploitability Metrics

Attack Vector (AV): Network (N) Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC): Low (L) High (H)

Attack Requirements (AT): None (N) Present (P)

Privileges Required (PR): None (N) Low (L) High (H)

User Interaction (UI): None (N) Passive (P) Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): High (H) Low (L) None (N)

Integrity (VI): High (H) Low (L) None (N)

Availability (VA): High (H) Low (L) None (N)

Changes to Base metrics

User Interaction

Base Metrics ?

Exploitability Metrics

Attack Vector (AV):

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC):

Low (L)

High (H)

Attack Requirements (AT):

None (N)

Present (P)

Privileges Required (PR):

None (N)

Low (L)

High (H)

User Interaction (UI):

None (N)

Passive (P)

Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC):

High (H)

Low (L)

None (N)

Integrity (VI):

High (H)

Low (L)

None (N)

Availability (VA):

High (H)

Low (L)

None (N)

Retired Metrics



-He? You came in with a she.
-One little mistake.

Retired Metrics

No more Scope metric!



Retired Metrics

Vulnerable System Impact Metrics			
Confidentiality (VC):	High (H)	Low (L)	None (N)
Integrity (VI):	High (H)	Low (L)	None (N)
Availability (VA):	High (H)	Low (L)	None (N)

Subsequent System Impact Metrics			
Confidentiality (SC):	High (H)	Low (L)	None (N)
Integrity (SI):	High (H)	Low (L)	None (N)
Availability (SA):	High (H)	Low (L)	None (N)

Assess the impact of vulnerable systems and “subsequent” systems directly with **VC/VI/VA** and **SC/SI/SA** Base Metrics

Retired Metrics

No more Temporal metric!

Temporal Score

Exploit Code Maturity (E)

Not Defined (X) Unproven (U) Proof-of-Concept (P) Functional (F) High (H)

Remediation Level (RL)

Not Defined (X) Official Fix (O) Temporary Fix (T) Workaround (W) Unavailable (U)

Report Confidence (RC)

Not Defined (X) Unknown (U) Reasonable (R) Confirmed (C)

Retired Metrics

- The Temporal metric has been renamed **Threat** metric, and has been simplified to a single value.

Threat Metrics ?

Exploit Maturity (E):

Not Defined (X)

Attacked (A)

POC (P)

Unreported (U)

New Scoring Nomenclature



Damage control is easy.
Reading Klingon, that's hard.

New Scoring Nomenclature

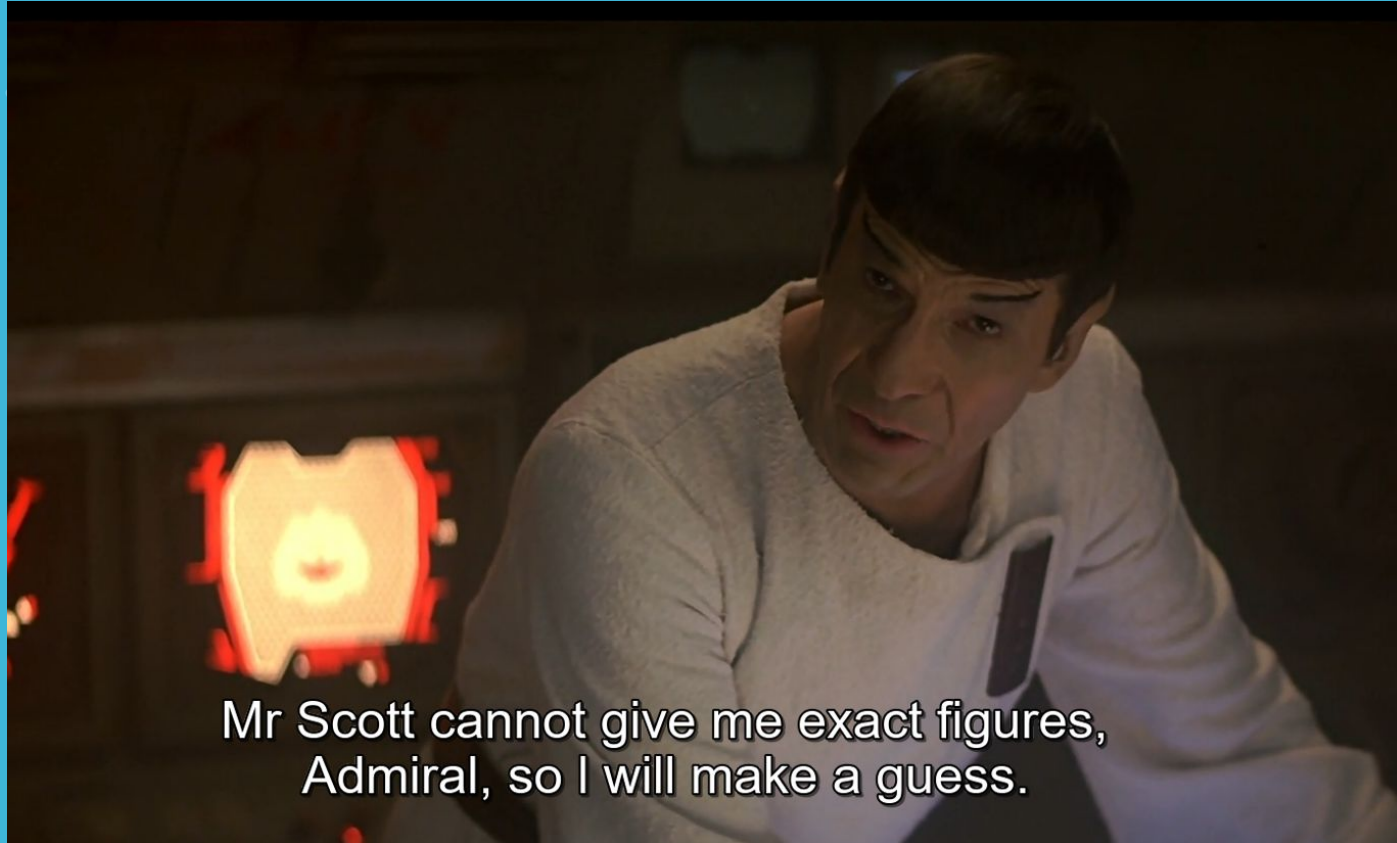
CVSS-B: CVSS base score

CVSS-BT: CVSS base + threat score

CVSS-BE: CVSS base + environmental score

CVSS-BTE: CVSS base + threat + environmental score

New: Supplemental Metrics



Mr Scott cannot give me exact figures,
Admiral, so I will make a guess.

New: Supplemental Metrics

Six new optional metrics, whose values are typically set by the vulnerable product's vendor, and which **do not affect the score**.

Supplemental Metrics ?

Safety (S):	Not Defined (X)	Negligible (N)	Present (P)		
Automatable (AU):	Not Defined (X)	No (N)	Yes (Y)		
Recovery (R):	Not Defined (X)	Automatic (A)	User (U)	Irrecoverable (I)	
Value Density (V):	Not Defined (X)	Diffuse (D)	Concentrated (C)		
Vulnerability Response Effort (RE):	Not Defined (X)	Low (L)	Moderate (M)	High (H)	
Provider Urgency (U):	Not Defined (X)	Clear	Green	Amber	Red

New focus on Safety



New focus on Safety

A new set of values under Environmental metrics allows scorers to describe a **Safety** impact, more severe than **High**, to the Integrity and Availability of a Subsequent System.

Subsequent System Impact Metrics

Confidentiality (MSC):

Not Defined (X)



High (H)

Low (L)

Negligible (N)

Integrity (MSI):

Not Defined (X)

Safety (S)

High (H)

Low (L)

Negligible (N)

Availability (MSA):

Not Defined (X)

Safety (S)

High (H)

Low (L)

Negligible (N)

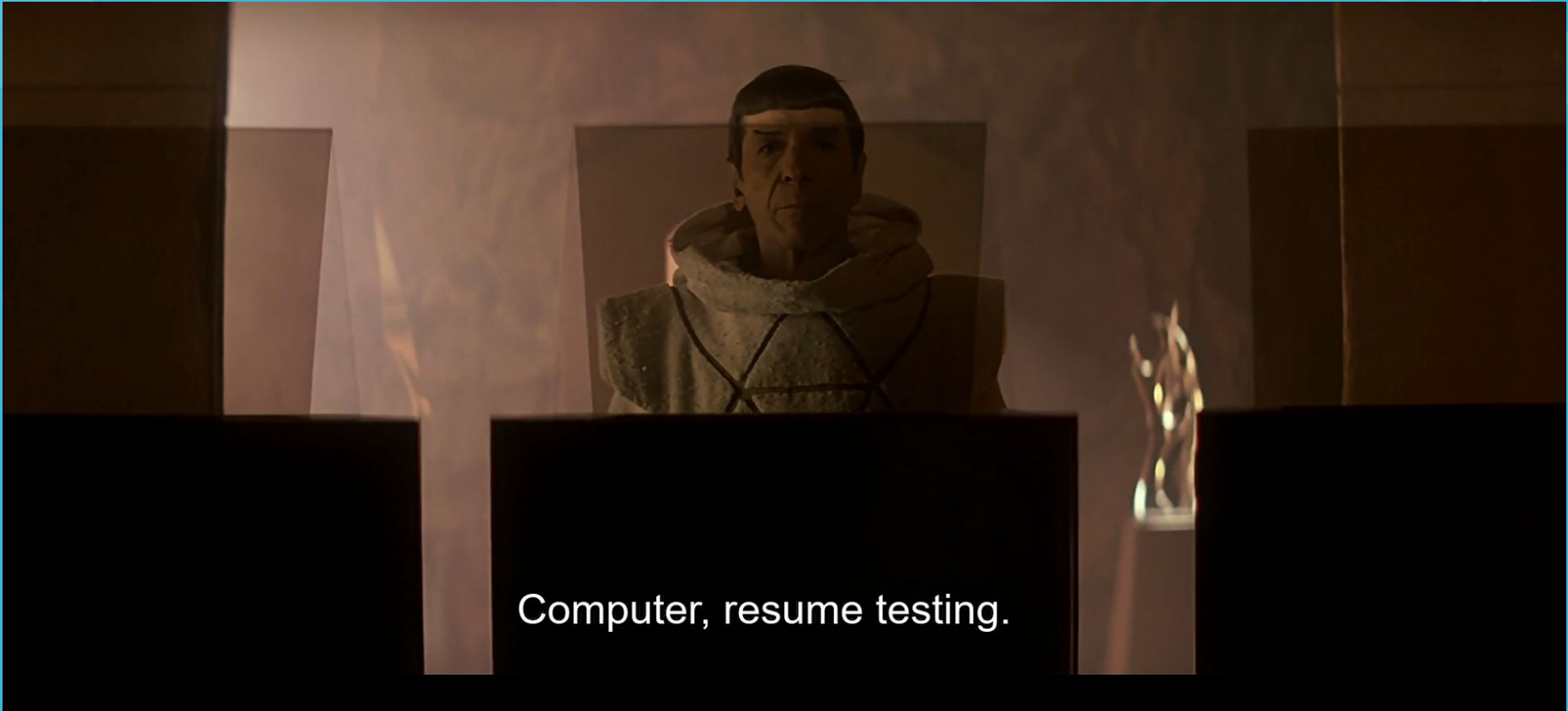
New focus on Safety

The Safety supplemental metric can be set by the vendor to
Negligible or **Present**.

Supplemental Metrics ?

 Safety (S):	Not Defined (X)	Negligible (N)	Present (P)		
Automatable (AU):	Not Defined (X)	No (N)	Yes (Y)		
Recovery (R):	Not Defined (X)	Automatic (A)	User (U)	Irrecoverable (I)	
Value Density (V):	Not Defined (X)	Diffuse (D)	Concentrated (C)		
Vulnerability Response Effort (RE):	Not Defined (X)	Low (L)	Moderate (M)	High (H)	
Provider Urgency (U):	Not Defined (X)	Clear	Green	Amber	Red

Scoring Examples



Computer, resume testing.

Scoring Example 1: Curl

CVE-2023-38545

This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.

CVSS-BT: 8.5

(CVSS 3.1 equiv: 8.8)

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/E:P

<https://www.first.org/cvss/calculator/4.0#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/E:P>

Scoring Example 2: Confluence

CVE-2023-22515

A vulnerability in publicly accessible Confluence Data Center and Server instances allows attackers to create unauthorized Confluence administrator accounts and access Confluence instances.

CVSS-BT: 9.3

(CVSS 3.1 equiv: 9.8)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A

CVSS-BTE: 9.2

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:L/MAT:P/MPR:N/MUI:N/MVC:H/MVI:H/MVA:H/MSA:N/MSI:N/MSA:N/S:N/AU:Y/R:U/V:C/RE:L/U:Red 🤪

Scoring Example 3: Siemens

CVE-2019-13946

Siemens Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface, causing a Denial of Service.

CVSS-BT: 7.7

(CVSS 3.1 equiv: 7.5)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

CVSS-BTE: 9.4

(with Vulnerable and Subsequent System
Availability Impact set to **Safety**)

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P/MVA:H/MSA:S

Resources

FIRST has specification docs, a user guide, and interactive training on CVSSv4:

first.org/cvss



Live long, and prosper.

Any questions?

@justinhall

