**Problem**: we need to standardize on vulnerability severity measurement / criteria

- Different orgs have different ideas as to what constitutes crit/high/etc
- High subjectivity
  - Many companies with immature security programs are like this
- May want a higher level of granularity than severity buckets
  - Is this high sev more or less urgent than that high sev?
Solution: Common Vulnerability Scoring System

- Open, widely accepted industry standard
  - Current revision 3.1 (June ’19)
- Assigns numeric score 0.0–10.0 based on various criteria
  - Scores are ±0.5 from ‘objective’ severity
  - Various equations translate criteria into scores
- Produces a string like this: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

Severity Levels:
- None (0.0)
- Low (0.1–3.9)
- Medium (4.0–6.9)
- High (7.0–8.9)
- Critical (9.0–10.0)
Why use CVSS?

• Otherwise severity criteria are not ‘objective’ — clients may push back
  • You might also not know how to rate a vulnerability
  • Can’t go wrong with arguing based on an industry-wide standard

• If you encounter a known vulnerability in the wild (e.g., reading CVE writeup),
  CVSS lets you:
  • Quickly assess general impact (High/med/low)
  • Specifically identify how it affects you
    • (Do I need physical access? Do I need privileges to exploit?)
## CVSS Subscores

### Base
- Main score people are familiar with
- Calculated in the **generic case**
  - “reasonable worst-case impact”
- Nearly always stops here
  - Scanners, etc.

### Temporal
- In general, goes up over time
- Considers:
  - Maturity of exploit code
  - Availability of patches/workarounds
  - Confidence in vulnerability
    - As in, confidence in the existence generally, not for you

### Environmental
- Only score that is based on your specific case
- Consider impact of vuln on your specific security requirements
- Considers specific ways the vuln applies to you

Temporal, Environmental scores produce modifiers for base score. Temporal score can only reduce the score; Environmental can increase or decrease.
Calculating CVSS Scores

Use a calculator:
https://www.first.org/cvss/calculator/3.1
CVSS Base Metrics

**Attack Vector:**
- Network — non-local network (e.g., Internet)
- Adjacent — same broadcast domain or local-only protocol (e.g., Bluetooth)
- Local — local access already (e.g., already have a shell)
- Physical — requires hands-on physical access, even briefly

**Attack Complexity:**
- Low — can easily be executed against a generic system
- High — requires target specific reconnaissance, specific circumstances, be a man-in-the-middle, etc.

**User Interaction:**
- None — works without any user action
- Required — requires some user action (includes “clicking on a phishing link”)
CVSS Base Metrics

Privileges Required:
• None — unauthenticated/pre-auth
• Low — low access (e.g., low priv user)
• High — high access (e.g., admin user)

Scope:
• Unchanged — affects the same system (e.g., go from low to high priv in a web app)
• Changed — affects a different system (e.g., escape sandbox, gain code execution on web server)
CVSS Base Metrics — CIA Triad

• Confidentiality: secrecy of sensitive information
  • E.g., PII, passwords, keys
• Integrity: non-modification of data
• Availability: system accessibility

Impact levels:
• None — no impact
• Low — limited impact, may not be controlled / reliable
• High — complete compromise, or compromise of extremely sensitive assets
Example: CSRF to RCE

Hypothetical

• Local CSRF on management page
• Requires user to click on a link
• Requires a valid local certificate
  • Requires attacker to also know the right hostname

CVSS Scoring?

https://www.first.org/cvss/calculator/3.1
CVSS Temporal Scoring

• All subscores can be “not defined” — don’t affect score in that case

• Temporal scores modify score based on age of vuln
  • Only modify downward
  • Generally idea is that it goes up over time

• “Better” metrics reduce CVSS
  • Makes sense — if there’s no public details for a vuln, less urgent than one that’s in Metasploit
CVSS Temporal Metrics

Exploit Maturity
- Unproven — no PoC
- Proof-of-Concept — PoC available but not weaponized or generalized
- Functional — Exploit code is available and works most of the time
- High — “one click” exploits available (e.g., Metasploit)

Remediation Level
- Official Fix — patched
- Temporary Fix — patched via hotfix or similar
- Workaround — can be fixed via e.g., config change to disable affected component
- Unavailable — no fix available

Report Confidence
- Unknown — reports are from unknown source with no confirmation; conflicting information available
- Reasonable — details available, but full root cause is unknown
- Confirmed — vendor has confirmed issue and impact

All subscores can be “not defined” — don’t affect score in that case
Example: CSRF to RCE

Hypothetical
- Local CSRF on management page
- Requires user to click on a link
- Requires a valid local certificate
  - Requires attacker to also know the right hostname

CVSS Scoring?

https://www.first.org/cvss/calculator/3.1
CVSS Environmental Subscoring

• Modifies the CVSS *up or down* based on your specific circumstances

• 3 additional metrics based on CIA requirements
  • E.g., if your environment uses an application for storing keys, it has a high confidentiality requirement
  • E.g., if your environment uses an application to store lunch orders, it has a low confidentiality requirement

• Also allows modified scores for all CVSS base scores
  • Used to represent how a system is used in your specific environment
  • E.g., if an application is behind a VPN, all bugs have a “low” modified privileges required metric at the minimum
Example: CSRF to RCE

Hypothetical

• Local CSRF on management page
• Requires user to click on a link
• Requires a valid local certificate
  • Requires attacker to also know the right hostname

CVSS Scoring?

https://www.first.org/cvss/calculator/3.1
Example: Admin Command Injection in Web app

Hypothetical
- Web app
- Admin interface has command injection
- PoC is available but not weaponized
  - Requires manual customization for each target
- Our environment has it behind a VPN
- We use it to store top secret proprietary data

CVSS Scoring?

https://www.first.org/cvss/calculator/3.1
Thank you!

Any questions?
More Information

• Calculator: https://www.first.org/cvss/calculator/3.1
• User Guide: https://www.first.org/cvss/v3.1/user-guide
• Examples: https://www.first.org/cvss/v3.1/examples
• Self-Guided Online Training: https://learning.first.org/courses/course-v1:FIRST+CVSSv3+2017/about
• Specification: https://www.first.org/cvss/v3.1/specification-document