Common Vulnerability Scoring System v2

Seth Hanford

CVSS-SIG v3 Chair

Agenda

- CVSS v2 Overview
- Scoring Criteria
- Caveats
- V3 Development
- Examples

Overview

What is CVSS?

- Common Vulnerability Scoring System

  Common system to convey vulnerability characteristics, assign Severity scoring, and help to determine Urgency and Priority of response

- Version 1 developed by NIAC, v2 developed under FIRST.org
- Development is iterative, driving CVSS toward a scoring model that reflects expert expectations for Severity, Urgency, Priority
- CVSS Special Interest Group: http://www.first.org/cvss
- CVSS v2 Scoring Guide: http://www.first.org/cvss/cvss-guide
- Work on v3 has begun

What is CVSS? cont.

- Purpose
  - Assign standard names to vulnerability characteristics
  - Derive scores from the combination of those characteristics
  - Prioritize response based upon those scores, among a diverse set of vulnerabilities, vendors, and environments
- Usage
  - Vendors
  - Government
  - Security scanning / assessment
  - Vulnerability Intelligence Services
- Descriptive value, not just scoring value

How vulnerabilities are scored

- Base score
  - Required
  - Static, once all information is available
  - Usually set by Vendor or Reporter; Vendor's score "wins"
- Temporal Score
  - Sometimes present
  - Dynamic, but progresses in one direction over vulnerability lifetime
  - Often provided by end user or intelligence service
- Environmental Score
  - Organizational responsibility
- Final Score (Metric)
  - At least a Base score; all Temporal and Environmental are optional
  - (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)

What you need

- The Guide: http://www.first.org/cvss/cvss-guide.pdf
- A CVSS calculator: http://www.first.org/cvss/scores
- A firm grasp of security terminology and common vulnerability characteristics
- Note: beware rounding errors; verify formula as presented in guide

Scoring Criteria

Base Metrics

Exploitability

- Access Vector (Network, Adjacent Network, Local)
- Access Complexity (Low, Medium, High)
- Authentication Required (None, Single, Multiple)

Impact

- Confidentiality (None, Partial, Complete)
- Integrity (None, Partial, Complete)
- Availability (None, Partial, Complete)

Scoring Base Metrics, Exploitability

- Access Vector (AV)
- Farthest position of the attacker, relative to a vulnerable target
- Network (N)
  - Remotely exploitable
  - System accepts via network stack (non UI)
- Adjacent Network (A)
  - Physical proximity (e.g. Bluetooth range)
  - Broadcast domain (e.g. same subnet; privileged network position)
- Local (L)
  - Physical, Console or UI Access
  - System accepts via interactive session

Scoring Base Metrics, Exploitability cont.

- Access Complexity (AC)
- Addresses the complexity of factors outside the attackers control
- High (H)
  - Elevated Privileges required by attacker
  - Highly unlikely exploit path (e.g. user unlikely to perform a very suspicious action)
- Medium (M)
  - Specific privileges required by attacker
  - Some factors outside attackers control (e.g. human intervention required by victim)
- Low (L)
  - Attacker fully controls the exploit path (e.g. vulnerable service listens by default)

Scoring Base Metrics, Exploitability cont.

- Authentication (Au)
- Attacker's required system credentials
- Multiple (M)
  - Two or more sets of credentials
- Single (S)
  - One set of credentials
- None (N)

Scoring Base Metrics, Impact

- Confidentiality (C)
  - Access to information resources
  - Read data, or loss of Access Control
- Integrity (I)
  - Modification of information resources
  - Write data, or loss of data integrity
- Availability (A)
  - Availability of information resources
  - System non-responsive, or system performance significantly degraded

Scoring Base Metrics, Impact cont.

- Each of C, I, A scored, relative to the Host, as:
- None (N)

  No loss to this Impact category
- Partial (P)

  Attacker is constrained in either Scope or Control
- Complete (C)

  Attacker is unconstrained in their impact to this category
- Note: If all of C, I and A are None, then CVSS = 0.0

Temporal Metrics

Exploitability

- Unproven
- Proof-of-concept
- Functional
- High
- Not Defined

Remediation Level

- Official Fix
- Temporary Fix
- Workaround
- None
- Not Defined

Report Confidence

- Unconfirmed
- Uncorroborated
- Confirmed
- Not Defined

Scoring Temporal Metrics

- Exploitability (E)
  - What is the public availability of example code which exploits the vulnerability?
- Not Defined (ND)
- Unproven (U)
  - Theoretical, no public demonstration
- Proof of Concept (POC)
  - Works for some platforms, or with limited impact
- Functional (F)
  - Works for all platforms, for greatest impact
- High (H)
  - Malicious code or No exploit needed

Scoring Temporal Metrics, cont.

- Remediation Level (RL)
  - What is the public availability of remediations for the vulnerability?
- Not Defined (ND)
- Unavailable (U)
  - There is no resolution which maintains necessary functionality
- Workaround (W)
  - Third-party solution which preserves functionality but limits exploitability
- Temporary Fix (TF)
  - Vendor supplied, non-final fix for the vulnerability
- Official Fix (OF)
  - Patch or official solution available from the vendor

Scoring Temporal Metrics, cont.

- Report Confidence (RC)
  - What is the degree of confidence in the vulnerability and its characteristics?
- Not Defined (ND)
- Unconfirmed (UC)
  - Low credibility or conflicting reports
- Uncorroborated (UR)
  - Medium credibility, non-official sources, some lingering ambiguity
- Confirmed (C)
  - Vendor supplied, official confirmation

Environmental Metrics

Collateral Damage Potential

- None
- Low
- Low-medium
- Medium-high
- High
- Not Defined

Target Distribution

- None
- Low
- Medium
- High
- Not Defined

Security Requirements

- Confidentiality (Low, Medium, High, Not Defined)
- Integrity (Low, Medium, High, Not Defined)
- Availability (Low, Medium, High, Not Defined)

Scoring Environmental Metrics

- Collateral Damage Potential (CDP)
  - Describes the impact to non-vulnerable systems in the event of a successful exploit
- Not Defined (ND) / None (N)
- Low (L)
  - Slight loss
- Low-Medium (LM)
  - Moderate loss
- Medium-High (MH)
  - Significant loss
- High (H)
  - Catastrophic loss

Scoring Environmental Metrics, cont.

- Target Distribution (TD)
  - Describes the occurrence of vulnerable systems within an environment
- Not Defined (ND)
- None (N) – CVSS = 0.0
- Low (L)
  - 1-25% of environment considered At Risk
- Medium (M)
  - 26-75% of environment considered At Risk
- High (H)
  - 76-100% of environment considered At Risk

Scoring Environmental Metrics, cont.

- Security Requirements (CR, IR, AR)
  - Describes the sensitivity of loss to C, I, and A
- Not Defined (ND)
- Low (L)
  - Limited impact
- Medium (M)
  - Serious impact
- High (H)
  - Catastrophic impact

Caveats

V2 Caveats

- Scoring in v2 is host-centric
  - Some vulnerabilities don't "score well" in this assumption
- Scoring Tips section of the v2 Guide assists with common difficulties
- Much of the work from v1 to v2 focused on Base Scoring
  - Temporal got little work
  - Environmental was changed, but only to move Base metrics to Environmental
  - Much of v2 scoring experience in industry is Base, with some Temporal

V3 Development

Call for Participants

- Opened March 19, 2012
- Accepting applications through May 4
- First official meetings for Annual Conference, June 2012 (Malta)
- Representative model from government, industry, vendors, academia, and more
- See CfP posting online: http://www.first.org/newsroom/releases/20120322
- If interested, contact me: seth@first.org

Call for Subjects

- Will open April 6
- Collecting public feedback on v2 and suggestions for improvement in v3
- Collection will occur through the start of the Malta kick-off meetings (approx. through June 16, 2012)
- Will accept input after that date, but this is the window for setting the scope / direction of v3
- Please submit ideas to: seth@first.org

Examples

XYZ Corp Web Server Buffer Overflow

- XYZ Corp Web Server version 8 contains a buffer overflow vulnerability that could allow a remote, unauthenticated attacker to execute arbitrary code with the privileges of the web server process. An attacker can exploit this vulnerability by submitting an overly-long POST request to an affected system.
- Exploit code for XYZ Web Server that demonstrates this vulnerability on ABC Linux (64-bit only) has been posted to Pastebin
- XYZ Corp has not yet verified that the code posted to Pastebin affects XYZ Web Server. By default, XYZ Web Server runs as root
- Your organization (a web hosting reseller) serves 80% of customer sites on XYZ Web Server v. 8; 30% of XYZ Web Server-using customers are on 64-bit Linux platforms

XYZ Web Server Buffer Overflow, cont.

- Base 10.0
  - AV: **Network**
  - AC: **Low**
  - Au: **None**
  - C: **Complete**
  - I: **Complete**
  - A: **Complete**
- Temporal 8.1
  - E: **POC**
  - RL: **Workaround**
  - RC: **Uncorroborated**
- Environmental 9.1
  - CDP: **High**
  - TD: **High**
  - CR: **Low**
  - IR: **Low**
  - AR: **High**

123 Corp Browser Plugin Buffer Overflow

- 123 Corp Browser plugin version 1 contains a buffer overflow vulnerability that could allow a remote, unauthenticated attacker to execute arbitrary code with the privileges of the web browser process. An attacker can exploit this vulnerability by convincing a user to visit a malicious web site that loads the vulnerable plugin with malicious content.
- No exploits have been made publicly available
- 123 Corp has released advisory 123C-0472 to address this, and has released plugin version 1.1 which corrects it
- Your organization believes most, if not all, user desktops run the 123 Corp Browser Plugin version 1. Non-user systems, probably not.

123 Corp Browser Plugin Overflow, cont.

- Base 9.3
  - AV: **Network**
  - AC: **Medium**
  - Au: **None**
  - C: **Complete**
  - I: **Complete**
  - A: **Complete**
- Temporal 6.9
  - E: **Unproven**
  - RL: **Official Fix**
  - RC: **Confirmed**
- Environmental 7.2
  - CDP: **Low**
  - TD: **High**
  - CR: **Med**
  - IR: **Med**
  - AR: **Med**

123 Corp Browser Plugin Overflow, cont.

- Base 6.8
  - AV: **Network**
  - AC: **Medium**
  - Au: **None**
  - C: **Partial**
  - I: **Partial**
  - A: **Partial**
- Temporal 5
  - E: **Unproven**
  - RL: **Official Fix**
  - RC: **Confirmed**
- Environmental 5.5
  - CDP: **Low**
  - TD: **High**
  - CR: **Med**
  - IR: **Med**
  - AR: **Med**

ABC Inc. Firewall ACL Bypass

- ABC Firewalls running firmware 6.4 and prior contain a vulnerability that allows an attacker to bypass access control lists on an affected system. Attackers sending malicious traffic can bypass established ACLs.
- No public exploit examples have been published
- ABC Inc. has confirmed this vulnerability and has issued version 6.5, which corrects this flaw.
- Your organization uses ABC Firewalls to protect datacenter hosts on all links from business partner connections

ABC Inc. Firewall ACL Bypass, cont.

- Base 5.0
  - AV: **Network**
  - AC: **Low**
  - Au: **None**
  - C: **Partial**
  - I: **None**
  - A: **None**
- Temporal 4.4
  - E: **High**
  - RL: **Official Fix**
  - RC: **Confirmed**
- Environmental 1.7
  - CDP: **Medium-High**
  - TD: **Low**
  - CR: **Not Defined**
  - IR: **Not Defined**
  - AR: **Not Defined**

ABC Inc. Firewall ACL Bypass, cont.

- Base 5.0
  - AV: **Network**
  - AC: **Low**
  - Au: **None**
  - C: **Partial**
  - I: **None**
  - A: **None**
- Temporal 4.4
  - E: **High**
  - RL: **Official Fix**
  - RC: **Confirmed**
- Environmental 6.6
  - CDP: **Medium-High**
  - TD: **High**
  - CR: **Not Defined**
  - IR: **Not Defined**
  - AR: **Not Defined**