Understanding the latest CVSS 4.0

www.thecyphere.com info@thecyphere.com

CVSS, the Common Vulnerability Scoring System, is a popular open industry standard for evaluating vulnerabilities to assess their impact.

A bit of history

- CVSS 1.0: Released in 2005
  - First version of CVSS
  - Based on two metric groups: **Exploitability and Impact**
- CVSS 2.0: Released in 2007
  - Added Temporal and Environmental metric groups
  - Made several other changes to improve the accuracy and usefulness of the CVSS score

- CVSS 3
  - Released in 2015
  - Based on three metric groups:
    - **Base**: Exploitability, Impact, and Scope
    - **Temporal**: Exploit code maturity, Remediation level, and Report confidence
    - **Environmental**: attacker prerequisites, user interaction, and availability requirements

- CVSS 3
  - Each metric is assigned a score from 0 to 10, with 10 being the most severe
  - The overall CVSS score is calculated using a formula that takes into account all of the metric scores

Notable changes in CVSS v4.0

- New nomenclature:
  - Base (CVSS-B), Base + Threat (CVSS-BT), Base + Environmental (CVSS-BE), and Base + Threat + Environmental (CVSS-BTE)
  - Base metrics: Attack Requirements, User Interaction.

- Enhanced impact disclosure: Vulnerable and Subsequent Systems.
- Renamed Temporal metrics to Threat metrics
- New Supplemental Metric Group
- Focus on OT/ICS/Safety
- Public Preview: June 8 - July 31, 2023
- Official publication : 1st Nov, 2023.

CVSS Groups and Metrics

- **Base:** Represents a vulnerability's intrinsic qualities, consistent across time and environments.
- **Threat:** Reflects a vulnerability's dynamic characteristics, changing over time.

- **Environmental:** Depicts a vulnerability's unique aspects within a user's environment.
- **Supplemental:** Add context by describing extrinsic vulnerability attributes.

Base metrics

(filled by supplier)

Exploitability Metrics

- Attack Vector (AV)
- Attack Complexity (AC)
- Attack Requirements (AT)
- Privileges Required (PR)
- User Interaction (UI)

Vulnerable system impact metrics

- Confidentiality (VC)
- Integrity (VI)
- Availability (VA)

Subsequent system impact metrics

- Confidentiality (SC)
- Integrity (SI)
- Availability (SA)

Supplemental metrics
(filled by supplier)

- Safety (S)
- Automatable (AU)
- Recovery (R)
- Value Density (V)
- Vulnerability Response Effort (RE)
- Provider Urgency (U)

Environmental

(filled by consumer)

Exploitability Metrics

- Attack Vector (MAV)
- Attack Complexity (MAC)
- Attack Requirements (MAT)
- Privileges Required (MPR)
- User Interaction (MUI)

Vulnerable system impact metrics

- Confidentiality (MVC)
- Integrity (MVI)
- Availability (MVA)

Subsequent system impact metrics

- Confidentiality (MSC)
- Integrity (MSI)
- Availability (MSA)

Environmental (Security requirements)

- Confidentiality Requirements (CR)
- Integrity Requirements (IR)
- Availability Requirements (AR)

Threat metrics

- Exploit Maturity (E)
  - It relates to the likelihood of a vulnerability being attacked (exploit availability, techniques)

CVSS Example

CVE-2022-41741

A vulnerability in ngx_http_mp4_module may let a local attacker corrupt NGINX worker memory, causing a termination or other damage using a crafted audio or video file.

You can read several such examples demonstrating various factors on first site

CVSS v3 Score: Base 7.0

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4 Score: Base 7.3

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

See the next slide what has changed

Attack requirements is the new metric

This issue impacts NGINX products built with ngx_http_mp4_module and using the mp4 directive in the configuration file. The attack is feasible when an attacker triggers the processing of the malicious audio or video file with the module.

Example specific metrics added in the next slides

Metric	Value	Comments
Attack Vector	Local	An attacker must be able to access the vulnerable system with a local, interactive session.
Attack Complexity	Low	No specialised conditions or advanced knowledge are required.

Metric	Value	Comments
Attack Requirements	Present	NGINX must be built with the module, and configuration must be present. Neither of those are default scenarios for an NGINX OSS web server. The attacker must place a file within the web root and cause NGINX to serve that file.
Privileges Required	Low	An attacker must be able to place a file within the web root to be processed by NGINX.

Metric	Value	Comments
User Interaction	None	No user interaction is required for an attacker to successfully exploit the vulnerability.
Vulnerable System Confidentiality	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Vulnerable System Integrity	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.

Metric	Value	Comments
Vulnerable System Availability	High	The attacker could execute arbitrary code on the vulnerable system with elevated privileges.
Subsequent System Confidentiality	None	There is no impact to the subsequent system confidentiality.
Subsequent System Integrity	None	There is no impact to the subsequent system integrity.
Subsequent System Availability	None	There is no impact to the subsequent system availability.

Liked this?

Share with others

Need a chat? Get in touch:

thecyphere.com

info@thecyphere.com