EnCyb

Severity: High

Advisory Type: Security

GNU Wget2 Arbitrary File Overwrite Vulnerability

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

A critical path traversal vulnerability in GNU Wget2 (CVE-2025-69194) allows attackers to overwrite arbitrary files via malicious Metalink files, posing a high risk of data loss and system compromise.

- CVE ID: CVE-2025-69194
- Active Region: Global
- Affected Sector: Information Technology / Software Development / DevOps
- Affected Product: GNU Wget2
- Severity: High
- CVSS: 8.8
- Published Date: January 5, 2026

TECHNICAL DETAILS

- Target: Linux and Unix-like systems using GNU Wget2, particularly servers and automated environments such as scripts and CI/CD pipelines with write access to sensitive directories.
- Root Cause: Improper validation and normalization of file paths in Metalink processing, allowing path traversal sequences (such as ../) to bypass directory restrictions and write files to unintended locations on the filesystem.
- Prerequisite For Exploitation: Exploitation requires a user or automated process to process a malicious Metalink file, with impact depending on the privileges of the Wget2 execution, potentially allowing overwriting of critical files and configurations.

IMPACT

- Arbitrary files overwrite on the affected system.
- Loss or corruption of critical system and user data.
- Potential local or remote code execution.
- Privilege escalation through modified configuration files.
- Service disruption or denial-of-service conditions.

RECOMMENDATIONS

- Avoid downloading or processing Metalink files from untrusted or unknown sources.
- Update GNU Wget2 to the latest available version as soon as patches are released.
- Do not run Wget2 with elevated privileges unless absolutely necessary.
- Review and secure scripts, automation, and CI/CD pipelines that rely on Wget2.
- Implement file system permission controls to limit write access to sensitive directories.

REFERENCE

- https://teamwin.in/critical-gnu-wget2-vulnerability-let-remote-attackers-to-overwrite-sensitive-files/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com