مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote Code Execution Vulnerability in Git Submodules

Tracking #:432315868

Date:20-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Remote Code Execution (RCE) vulnerability in Git submodules that can be used to gain remote code execution (RCE) during a “clone” operation.

TECHNICAL DETAILS:

- **CVE ID:CVE-2024-32002**
- This vulnerability allows attackers to create malicious Git repositories with submodules. When a user clones such a repository, Git can be tricked into writing files to unintended locations, specifically the .git/ directory. This can lead to remote code execution (RCE) without the user's knowledge or consent.
- Proof of Concept (PoC) for CVE-2024-32002, a Remote Code Execution (RCE) vulnerability exists.
- **Affected Versions**: Git versions v2.45.0 v2.44.0 <=v2.43.3 <=v2.42.1 v2.41.0 <=v2.40.1 <=v2.39.3
- **Updated Versions**: Git v2.45.1, v2.44.1, v2.43.4, v2.42.2, v2.41.1, v2.40.2, and v2.39.4
- Disabling symbolic link support in Git can also mitigate this vulnerability and avoid cloning repositories from untrusted sources.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to fixed version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://github.com/git/git/security/advisories/GHSA-8h77-4q3w-gfgv