Security Advisory 2024-046

Multiple Vulnerabilities in Git

May 22, 2024 — v1.0

TLP:CLEAR

History:

- *22/05/2024 — v1.0 – Initial publication*

Summary

On May 14, 2024, GitHub announced the release of Git version 2.45.1, addressing three critical vulnerabilities impacting multiple platforms, including Windows, macOS, Linux, and BSD [1,2]. These vulnerabilities could allow for remote code execution and unauthorised file modifications.

Technical Details

The vulnerability `CVE-2024-32002`, with a CVSS score of 9.1, could allow a remote attacker to execute code on the affected device. To do so, an attacker would need to craft repositories with submodules in a way that exploits a bug in Git whereby it can be fooled into writing files not into the submodule's worktree but into a `.git/` directory. This allows writing a hook that will be executed while the clone operation is still running, giving the user no opportunity to inspect the code that is being executed. [3]

The vulnerability `CVE-2024-32004`, with a CVSS score of 8.2, could allow an attacker, on multi-user machines, to create a local repository that appears as a partial clone that is missing an object. Then, when this repository is cloned, it causes Git to execute arbitrary code with the full permissions of the user performing the clone. [4]

The vulnerability `CVE-2024-32465`, with a CVSS score of 7.4, could allow an attacker to bypass protections for cloning untrusted repositories. While this vulnerability has been covered in CVE-2024-32004, there are circumstances where the fixes for CVE-2024-32004 are not enough, e.g., when obtaining a `.zip` file containing a full copy of a Git repository, it should not be trusted by default to be safe, as e.g., hooks could be configured to run within the context of that repository. [5]

Affected Products

All Git installations prior to version 2.45.1 across Windows, macOS, Linux, and BSD platforms are affected by these vulnerabilities.

Recommendations

It is strongly recommended upgrading to a fixed version immediately. Users unable to upgrade should exercise caution when cloning repositories, especially from untrusted sources.

References

[1] https://github.blog/2024-05-14-securing-git-addressing-5-new-vulnerabilities/

[2] https://github.com/git/git/security/advisories

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

[4] https://github.com/git/git/security/advisories/GHSA-xfc6-vwr8-r389

[5] https://github.com/git/git/security/advisories/GHSA-vm9j-46j9-qvq4