Mphasis
The Next Applied

Git patches two critical remote code execution security flaws

Severity: High

Date: 24th Jan 2023

Description

Git has patched two critical severity security vulnerabilities that could allow attackers to execute arbitrary code after successfully exploiting heap-based buffer overflow weaknesses.

Methodology

A third Windows-specific flaw impacting the Git GUI tool caused by an untrusted search path weakness enables unauthenticated threat actors to run untrusted code low-complexity attacks.

The first two vulnerabilities (CVE-2022-41903 in the commit formatting mechanism and CVE-2022-23521 in the .gitattributes parser) were patched on Wednesday in new versions going back to v2.30.7.

The third one, tracked as CVE-2022-41953, is still waiting for a patch, but users can work around the issue by not using the Git GUI software to clone repositories or avoid cloning from untrusted sources.

Impact

Security experts from X41 (Eric Sesterhenn and Markus Vervier) and GitLab (Joern Schneeweisz) found these vulnerabilities as part of a security source code audit of Git sponsored by OSTIF.

"The most severe issue discovered allows an attacker to trigger a heap-based memory corruption during clone or pull operations, which might result in code execution. Another critical issue allows code execution during an archive operation, which is commonly performed by Git forges," X41 security experts said.

Additionally, a huge number of integer related issues was identified which may lead to denial-of-service situations, out-of-bound reads or simply badly handled corner cases on large input."

Package	Affected versions	Patched versions
git-for-windows	<=2.39.0(2)	>=2.39.1

Mitigation

In all cases, the most effective way to defend against attacks attempting to exploit these vulnerabilities is to upgrade to the latest Git release (v2.39.1).

Users who cannot immediately update to address the CVE-2022-41903 critical remote code execution bug can also take the following measures to ensure that attackers cannot abuse the vulnerable Git functionality:

- Disable 'git archive' in untrusted repositories or avoid running the command on untrusted repos
- If 'git archive' is exposed via 'git daemon,' disable it when working with untrusted repositories by running the 'git config --global daemon.uploadArch false' command

We strongly recommend that all installations running a version affected by the issues are upgraded to the latest version as soon as possible.

Reference Links

https://www.bleepingcomputer.com/news/security/git-patches-two-critical-remote-code-execution-security-flaws/

Copyright © Mphasis Corporation. All rights reserved.