Security Advisory 2023-002

Multiple critical Vulnerabilities in Git

January 19, 2023 — v1.0

TLP:CLEAR

History:

- *19/01/2023 — v1.0 – Initial publication*

Summary

During a code audit [1], X41 discovered several vulnerabilities in the version control system `git`. On January 17, the `git` project resolved the two most critical security vulnerabilities (CVE-2022-23521 and CVE-2022-41903) that could allow the remote execution of arbitrary code. GitHub and GitLab have also issued updates for their products, including the latest version of `git`. A third vulnerability (CVE-2022-41953) affects the Windows version of the `Git GUI` software and could also lead to the execution of arbitrary code.

CERT-EU highly recommend upgrading to the latest version of `git`. In addition, if you are running on-premise GitHub or GitLab servers, we recommend updating them [2,3,4].

Technical Details

CVE-2022-23521

Using its `log` subcommand, `git` can display commits in an arbitrary format (`--format` specifiers). Additionally, `git` exposes this functionality also through `git archive` using the `export-subst` gitattribute.

When processing the padding operations, e.g., `%<(`, `%<|(`, `%>(`, `%>>(`, or `%><(`, an integer overflow can occur. This overflow can result in arbitrary heap writes, which may result in remote code execution. Users can trigger this behaviour by running a command that uses commit formatting, like `git log --format=...`. Indirectly an attacker can trigger the overflow through `git archive` via the `export-subst` mechanism. This command expands format specifiers inside files within the repository during a `git archive` [5].

CVE-2022-41903

`git` uses gitattributes to define attributes for paths. Users can define these attributes by adding a `.gitattributes` file to the repository. This file contains a set of file patterns and the attributes that `git` should set for matching paths.

Multiple integer overflows can occur when `git` parses a huge number of patterns, a huge number of attributes for a single pattern, or when the declared attribute names are huge. An attacker can trigger these overflows via a crafted `.gitattributes` file that may be part of the

commit history. The failure depends on whether the file exists in the working tree, the index, or both. `git` splits lines longer than 2KB when parsing gitattributes from files but not when parsing them from the index.

In the latter case, the overflow can result in arbitrary heap reads and writes, which may result in remote code execution [6].

CVE-2022-41953

Git GUI is a graphical tool bundled with Git for Windows. After cloning a repository, Git GUI will automatically post-process it. This post-processing includes, if available, running a spell checker called `aspell.exe`. Unfortunately, due to the use of Tcl/Tk as a GUI framework, the path to search for an executable *will always include the current directory*. Therefore, Git GUI could execute a malicious `aspell.exe` in the top-level directory of a cloned repository without leaving the user a chance to inspect it first and run potentially untrusted code on the local system [7].

Affected Products

- git-for-windows
  - affected versions: <=2.39.0(2)
  - patched versions: >=2.39.1
- git
  - affected versions: <= v2.30.6, v2.31.5, v2.32.4, v2.33.5, v2.34.5, v2.35.5, v2.36.3, v2.37.4, v2.38.2, v2.39.0
  - patched versions: >= v2.30.7, v2.31.6, v2.32.5, v2.33.6, v2.34.6, v2.35.6, v2.36.4, v2.37.5, v2.38.3, v2.39.1
- GitLab CE/EE
  - affected versions: < 15.7.4, 15.6.5, 15.5.8
  - patched versions: >= 15.7.5, 15.6.6, 15.5.9
- Github Enterprise Server
  - affected versions: < 3.3.19, 3.4.14, 3.5.11, 3.6.7, 3.7.4
  - patched versions: >= 3.3.19, 3.4.14, 3.5.11, 3.6.7, 3.7.4

Recommendations

CERT-EU very strongly recommends that all installations running an affected version are upgraded to the latest version as soon as possible. If you cannot upgrade you can use the following workarounds:

- CVE-2022-23521
  - Disable `git archive` in untrusted repositories;
  - If you expose `git archive` via `git daemon`, disable it by running `git config -global daemon.uploadArch`
  - Avoid running `git archive` directly on untrusted repositories.
- CVE-2022-41903
  - Avoid cloning from untrusted sources.
- CVE-2022-41953
  - Avoid using Git GUI for cloning. If that is not a viable option, at least avoid cloning from untrusted sources.

References

[1] https://github.com/git/git/files/10430260/X41-OSTIF-Gitlab-Git-Security-Audit-20230117-public.pdf

[2] https://about.gitlab.com/releases/2023/01/17/critical-security-release-gitlab-15-7-5-released/

[3] https://github.blog/2023-01-17-git-security-vulnerabilities-announced-2/

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

[5] https://github.com/git/git/security/advisories/GHSA-475x-2q3q-hvwq

[6] https://github.com/git/git/security/advisories/GHSA-c738-c5qq-xg89

[7] https://github.com/git-for-windows/git/security/advisories/GHSA-v4px-mx59-w99c