Security Policy

Reporting a vulnerability

Please send a detailed mail to git-security@googlegroups.com to report vulnerabilities in Git.

Even when unsure whether the bug in question is an exploitable vulnerability, it is recommended to send the report to git-security@googlegroups.com (and obviously not to discuss the issue anywhere else).

Vulnerabilities are expected to be discussed *only* on that list, and not in public, until the official announcement on the Git mailing list on the release date.

Examples for details to include:

- Ideally a short description (or a script) to demonstrate an exploit.
- The affected platforms and scenarios (the vulnerability might only affect setups with case-sensitive file systems, for example).
- The name and affiliation of the security researchers who are involved in the discovery, if any.
- Whether the vulnerability has already been disclosed.
- How long an embargo would be required to be safe.

Supported Versions

There are no official "Long Term Support" versions in Git. Instead, the maintenance track (i.e. the versions based on the most recently published feature release, also known as ".0" version) sees occasional updates with bug fixes.

Fixes to vulnerabilities are made for the maintenance track for the latest feature release and merged up to the in-development branches. The Git project makes no formal guarantee for any older maintenance tracks to receive updates. In practice, though, critical vulnerability fixes are applied not only to the most recent track, but to at least a couple more maintenance tracks.

This is typically done by making the fix on the oldest and still relevant maintenance track, and merging it upwards to newer and newer maintenance tracks.

For example, v2.24.1 was released to address a couple of CVEs, and at the same time v2.14.6, v2.15.4, v2.16.6, v2.17.3, v2.18.2, v2.19.3, v2.20.2, v2.21.1, v2.22.2 and v2.23.1 were released.