Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Git Integer Truncation Flaw Enables Code Execution During Recursive Clones

Date of Publication	Admiralty Code	TA Number
November 16, 2026	A1	TA2026339

Summary

First Seen: November 10, 2026
Affected Products: Git, GitHub Enterprise Server, applications bundling vulnerable Git builds
Impact: Successful exploitation grants an attacker arbitrary code execution in the context of the user or service account performing the recursive clone, which places developer workstations, CI/CD runners, build servers, and platforms that process repositories on behalf of users squarely in scope. Because these environments routinely hold source code, signing keys, cloud credentials, package-registry tokens, and deployment secrets, a single compromised clone can serve as a foothold for credential theft, tampering with build outputs, and onward software supply chain compromise. The attack requires only that a victim or automated pipeline recursively clone an attacker-controlled repository, a routine developer action that is easy to induce through social engineering or by embedding malicious repositories as submodules, which makes the business risk significant for any organization with a software development footprint until patched Git versions are deployed across endpoints, automation, and Git-bundling applications.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-111760	Git Integer Truncation Vulnerability	Git Project Git	✗	✗	✓

Vulnerability Details

#1 CVE-2026-111760 is a code execution vulnerability that allows a malicious repository to run arbitrary code on a victim's system. It affects Git's file checkout process, where Git validates each file path before writing it to the working directory and blocks any write that would overwrite protected internal metadata, most notably the `.git` entry that defines where a repository or submodule stores its configuration and history. The flaw lets an attacker bypass this validation. The vendor has not confirmed a CWE classification; based on the documented root cause, the issue maps to CWE-197 (Numeric Truncation Error).

#2 The flaw sits in Git's index, which records each file's path and its length. When a path is extremely long, the stored length is truncated. Git validates the full, harmless-looking path but writes the file under the shorter, truncated name, so an attacker can pick a long path that shortens to exactly the location Git is meant to protect.

#3 An attacker publishes a repository with a submodule and a path sized to collapse onto that submodule's `.git` file. When a developer or build system clones it with `--recurse-submodules`, Git writes a symbolic link in place of that file, pointing to an attacker-controlled directory that holds malicious configuration or hook scripts.

#4 Git then treats the attacker's directory as the submodule's repository and acts on its contents, running attacker-controlled code with the privileges of the account that performed the clone. The victim needs to do nothing beyond the clone itself.

#5 Fixes exist only for Git 2.56.1 and the 2.50 through 2.55 series (2.55.1, 2.54.1, 2.53.1, 2.52.1, 2.51.3, 2.50.2). No fix exists for Git 2.49 or earlier; users on those versions must move to a supported series. The fix rejects extremely long index paths before truncation and adds overflow checks to related memory allocations.

#6 GitHub has patched github.com, GitHub Enterprise Cloud, and GitHub Enterprise Cloud with data residency, and has released GitHub Enterprise Server 3.19.15, 3.20.11, 3.21.9, and 3.22.4. Patched GitHub Desktop and GitHub Copilot app releases are being coordinated, and GitHub Codespaces and GitHub Actions will also receive patched Git. Treat any other application that bundles Git as affected until its vendor confirms an update.

#7

The Git project rates the flaw CVSS v3.1 8.0 (High): network attack vector, high attack complexity, low privileges required, user interaction required, and changed scope. It considers the flaw triggerable only through clones that use --recurse-submodules. That offers little comfort: recursive cloning is routine in developer and build pipelines, on systems that hold source code, signing keys, and deployment credentials.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-111760	Git Project Git (Before 2.56.1, 2.55.1, 2.54.1, 2.53.1, 2.52.1, 2.51.3, 2.50.2)	cpe:2.3:a:git-scm:git:*:*:*:*:*:*:*:*	CWE-197 (analyst-mapped; not vendor-confirmed)
	GitHub Enterprise Server (Before 3.19.15, 3.20.11, 3.21.9, 3.22.4)	cpe:2.3:a:github:enterprise_server:*:*:*:*:*:*:*:*	

Recommendations

Upgrade Git Immediately: Update all Git installations to Git 2.56.1, or to the patched release for the maintenance series in use (2.55.1, 2.54.1, 2.53.1, 2.52.1, 2.51.3, or 2.50.2); systems on Git 2.49 or earlier have no fix and must move to a supported series. Use the operating system package manager or the official Git distribution. Updating is the most effective way to eliminate the vulnerability, and it should be prioritized on developer workstations and on any system that clones external repositories.

Upgrade GitHub Enterprise Server: Administrators of GitHub Enterprise Server should upgrade to versions 3.19.15, 3.20.11, 3.21.9, or 3.22.4, according to the release series deployed, as soon as possible. Schedule the upgrade as an emergency change where internal processes allow, since the server processes repository content on behalf of many users.

Update Applications That Bundle Git: Identify and update applications that ship their own copy of Git, such as GitHub Desktop, the GitHub Copilot app, IDEs, and Git GUI clients, because updating the system Git does not patch these bundled copies. Track vendor announcements for the coordinated GitHub Desktop and GitHub Copilot app releases and deploy them once available.

Patch Automation and Build Infrastructure: Update Git on CI/CD runners, self-hosted GitHub Actions runners, build servers, container base images, and any service that clones or processes repositories on behalf of users. Rebuild and redeploy container images that embed Git so that ephemeral build environments do not reintroduce vulnerable versions.

Restrict Recursive Clones of Untrusted Repositories: Until patches are fully deployed, clone only from trusted servers and avoid using `--recurse-submodules` on repositories from untrusted or unverified sources. Review scripts, pipeline definitions, and Git configuration for settings that enable submodule recursion by default, and disable them where they are not required, recognizing that these precautions reduce exposure but do not replace installing the fixes.

Inspect Recently Cloned Repositories: Review repositories recently cloned from external sources for submodules whose `.git` entry is a symbolic link rather than a regular file or directory, and for unexpected hook scripts or configuration changes. Treat any such finding as a potential compromise, isolate the affected system, and rotate credentials that were accessible to the user or service account that performed the clone.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.001: Compromise Software Dependencies and Development Tools
Execution	T1203: Exploitation for Client Execution	
	T1204: User Execution	
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1546: Event Triggered Execution	
Defense Evasion	T1211: Exploitation for Defense Evasion	

Patch Links

https://github.com/git/git/blob/v2.56.1/Documentation/RelNotes/2.56.1.adoc

https://github.com/git/git/security/advisories/GHSA-vp2w-7xxj-jvxr

https://git-scm.com/downloads

References

https://github.blog/open-source/git/git-security-vulnerabilities-announced-7/

https://github.com/git/git/security/advisories/GHSA-vp2w-7xxj-jvxr

https://lore.kernel.org/git/xmqqh5hosgw5.fsf@gitster.g/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 16, 2026 • 09:07 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com