Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Gitea RCE (CVE-2026-60004) Exploited to Hijack Servers for Crypto Mining

Date of Publication	Admiralty Code	TA Number
August 27, 2026	A1	TA2026249

Summary

First Seen: July 2026
Affected Products: Gitea
Impact: CVE-2026-60004 is a critical remote code execution flaw in Gitea, the widely used open-source, self-hosted Git platform. The weakness lives in Gitea's diffpatch API endpoint, which applies user-supplied patches inside a temporary Git repository. By submitting a specially crafted patch, an attacker with repository write access can plant an executable post-index-change Git hook that Git then runs, executing arbitrary shell commands as the Gitea service account. Because Gitea ships with open registration enabled by default, an external attacker can often meet the write-access requirement simply by creating an account and a repository, with no stolen credentials required. Confirming in-the-wild abuse, and at least one publicly reported intrusion used the flaw to drop a cryptocurrency-miner-like payload. No threat actor has been publicly attributed. Organizations running any affected version should upgrade to Gitea 1.27.1 immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-60004	Gitea Code Injection Vulnerability	Gitea	✗	✓	✓

Vulnerability Details

#1

Attackers are actively exploiting a critical-severity vulnerability in the Gitea self-hosted Git service, tracked as CVE-2026-60004. It stems from the way Gitea's diffpatch endpoint handled the temporary Git repository used to process incoming patches. Vulnerable releases built that workspace as a bare clone, in which the repository directory itself doubles as Git's internal data directory, the location where Git hooks are stored. When a patch is applied, Gitea runs a Git apply operation with a three-way merge fallback. Submitting the same patch twice creates an add/add collision, and Git's fallback writes the conflicting file into the checked-out path even though the operation targets the index. In a bare clone that path resolves inside the Git directory, so an executable file named hooks/post-index-change lands exactly where Git expects a live hook. Git then invokes it while writing the index, and the attacker's content runs as the Gitea service account.

#2

The vulnerable API call requires an authenticated user with repository write permission, but in practice that bar is low. Gitea's default configuration enables self-registration, frequently without administrator approval or email confirmation, and lets new users create repositories. An external attacker can therefore register, create a repository, and reach the diffpatch endpoint over HTTPS. That is precisely the path described in the one publicly reported intrusion, where the server's SSH was never exposed and the attack arrived entirely over the web interface.

#3

Every Gitea release from 1.17 up to but not including 1.27.1 is affected. Exploitation also depends on a few server-side conditions: a Git version new enough to support the relevant three-way fallback behavior (2.32 or later), an enabled diffpatch route, and a temporary filesystem where the Gitea service can both write and execute files. These conditions mean not every vulnerable instance is exploitable through the identical chain, but default deployments frequently line up.

#4

Notably, CVE-2026-60004 was not exploited as a zero-day. The patch shipped in late July, and confirmed abuse surfaced roughly a month afterward. Separately, an administrator publicly documented an intrusion in which an unknown actor exploited the flaw over HTTPS to run a dropper that behaved like a cryptocurrency miner, driving CPU usage high enough that the hosting provider throttled the server. The payload was never fully analyzed, so it is best described as miner-like rather than tied to a named family. Given the confirmed exploitation, the availability of a public proof-of-concept, and code execution as the Gitea service account, organizations running any affected version should upgrade to Gitea 1.27.1 immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-60004	Gitea (1.17 through 1.27.0, before 1.27.1)	cpe:2.3:a:gitea:gitea:*:*:*:*:*:*:*:*:*	CWE-94

Recommendations

Patch to Gitea 1.27.1 or Later Immediately: Upgrade every self-hosted Gitea instance to version 1.27.1 or newer without waiting for a routine maintenance window. This release fixes the flaw by processing patches in a non-bare temporary repository, so attacker-controlled content can no longer be interpreted as an executable Git hook. Gitea Cloud instances were slated to update automatically, but self-managed servers are the operator's responsibility.

Disable Open Registration Where It Is Not Needed: If you cannot patch right away, switch registration to administrator-controlled mode so an anonymous internet visitor cannot simply create an account and repository to gain the write access the exploit requires. This shrinks the attack surface but is not a fix, because existing users with write permissions can still reach the vulnerable functionality, so treat it strictly as a stopgap.

Reduce Exposure of Development Infrastructure: Restrict repository creation and write permissions to the users who genuinely need them, place Gitea behind a VPN or equivalent access controls, and avoid exposing self-hosted development platforms directly to the internet unless there is a clear business requirement. Every layer between an attacker and the `diffpatch` endpoint lowers the odds of opportunistic compromise.

Hunt for Signs of Exploitation: Because abuse is confirmed in the wild and no authoritative indicators of compromise have been published, review telemetry for behavioral evidence. Watch for unexpected requests to the `diffpatch` API, newly registered accounts that immediately create repositories and issue patch operations, unfamiliar processes or shells spawned by the Gitea service account, sustained high CPU usage, and unexpected downloads or outbound connections from the Gitea host or its child processes.

Treat a Suspected Compromise as Host-Level: If exploitation is suspected, assume the entire host is affected, since the attacker gained code execution as the Gitea service user. Rotate database credentials, OAuth and API tokens, CI/CD secrets, SSH keys, and deployment credentials reachable from the server, review private repositories for unauthorized changes, and examine connected build and deployment systems for lateral movement.

Vulnerability Management: Maintain an accurate inventory of Gitea deployments and their exact versions, subscribe to vendor security advisories, and fold internet-facing development tooling into a risk-based patching program so the next critical flaw in this class is identified and remediated quickly.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1136: Create Account	
Execution	T1059: Command and Scripting Interpreter	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://blog.gitea.com/release-of-1.27.1/

References

https://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m

https://github.com/0xBlackash/CVE-2026-60004

https://habr.com/ru/articles/1072030/

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

August 27, 2026 • 08:30 AM

More at www.hivepro.com