مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Remote Code Execution Vulnerability in GitHub

Tracking #:432318862

Date:30-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical command injection vulnerability, tracked as CVE-2026-3854, has been disclosed affecting GitHub and GitHub Enterprise Server (GHES).

TECHNICAL DETAILS:

A critical command injection vulnerability, tracked as CVE-2026-3854, has been disclosed affecting GitHub and GitHub Enterprise Server (GHES). The flaw allows an authenticated attacker with repository push access to achieve remote code execution (RCE) using a single git push command.
The vulnerability arises from improper sanitization of user-supplied git push options, which are embedded into internal service headers. Exploitation can lead to full compromise of affected instances, including cross-tenant data exposure in GitHub.com's multi-tenant environment.

Vulnerability Overview

- **Type:** Command Injection / Improper Input Neutralization
- **CVE ID:** CVE-2026-3854
- **CVSS Score:** 8.7 (High)
- **Attack Vector:** Network
- **Privileges Required:** Low (push access to repository)
- **User Interaction:** None

Affected Platforms

- GitHub.com
- GitHub Enterprise Cloud (all variants)
- GitHub Enterprise Server (GHES)

Root Cause

- User-controlled git push option values were:
  - Not properly sanitized
  - Embedded into internal X-Stat headers
- Internal header parsing relied on semicolon (;) delimiters
- Attackers could inject malicious metadata fields by crafting input containing delimiter characters

Patched Versions:

- GitHub Enterprise Server 3.14.25 or later
- GitHub Enterprise Server 3.15.20 or later
- GitHub Enterprise Server 3.16.16 or later
- GitHub Enterprise Server 3.17.13 or later
- GitHub Enterprise Server 3.18.7 or later
- GitHub Enterprise Server 3.19.4 or later
- GitHub Enterprise Server 3.20.0 or later

RECOMMENDATIONS:

Immediate Actions

- Upgrade GHES immediately to a patched version
- Verify patch levels across all instances

- Apply emergency patching if running exposed environments

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2026-3854