An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2604300225

NCSC Advisory

Critical RCE Vulnerability in GitHub Enterprise Server

CVE-2026-3854

30th, April 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Rialtas na hÉireann
Government of Ireland

Description

CVE ID: CVE-2026-3854

Published: 2026-03-10

Vendor: GitHub

Product: Enterprise Server

CVSS Score[1]: 8.7

Products Affected

Product	Version
Enterprise Server	3.14.0 <= 3.14.24
Enterprise Server	3.15.0 <= 3.15.19
Enterprise Server	3.16.0 <= 3.16.15
Enterprise Server	3.17.0 <= 3.17.12
Enterprise Server	3.18.0 <= 3.18.6
Enterprise Server	3.19.0 <= 3.19.3

Impact

An improper neutralization of special elements vulnerability was identified in GitHub Enterprise Server that allowed an attacker with push access to a repository to achieve remote code execution on the instance. During a git push operation, user-supplied push option values were not properly sanitized before being included in internal service headers.

Because the internal header format used a delimiter character that could also appear in user input, an attacker could inject additional metadata fields through crafted push option values. This vulnerability was reported via the GitHub Bug Bounty program and has been fixed in GitHub Enterprise Server versions 3.14.25, 3.15.20, 3.16.16, 3.17.13, 3.18.7 and 3.19.4.

[1] https://www.first.org/cvss/

Common Weakness Enumeration (CWE)[2]: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from GitHub.

- https://nvd.nist.gov/vuln/detail/CVE-2026-3854
- https://www.cve.org/CVERecord?id=CVE-2026-3854
- https://docs.github.com/en/enterprise-server@3.14/admin/release-notes#3.14.25
- https://docs.github.com/en/enterprise-server@3.15/admin/release-notes#3.15.20
- https://docs.github.com/en/enterprise-server@3.16/admin/release-notes#3.16.16
- https://docs.github.com/en/enterprise-server@3.17/admin/release-notes#3.17.13
- https://docs.github.com/en/enterprise-server@3.18/admin/release-notes#3.18.7
- https://docs.github.com/en/enterprise-server@3.19/admin/release-notes#3.19.4
- https://www.wiz.io/blog/github-rce-vulnerability-cve-2026-3854

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog