

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in GitHub Enterprise Server
Tracking #:432318021
Date:17-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in GitHub Enterprise Server allows attackers to execute malicious scripts through the web interface, potentially leading to privilege escalation and unauthorized actions.

TECHNICAL DETAILS:

Vulnerability Description

- **CVE-2025-11892**
- CVSS v3.1 Score: 8.6 (High)
- Type: DOM-based Cross-Site Scripting (XSS)
- An improper neutralization of input occurs in the Issues search label filter of GitHub Enterprise Server. This allows an attacker to inject malicious scripts into the web page. If a user with sudo privileges clicks a specially crafted link, the attacker could execute actions that normally require elevated permissions, including triggering workflows or modifying repository settings.
- Successful exploitation of this vulnerability can lead to privilege escalation, unauthorized workflow triggers, and execution of actions requiring elevated permissions.

Affected Versions

- GitHub Enterprise Server versions prior to:
 - 3.18.1
 - 3.17.7
 - 3.16.10
 - 3.15.14
 - 3.14.19

Fixed Versions

- GitHub Enterprise Server:
 - 3.18.1 and later
 - 3.17.7 and later
 - 3.16.10 and later
 - 3.15.14 and later
 - 3.14.19 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by GitHub.

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://www.cve.org/cverecord?id=CVE-2025-11892>