CVE-2024-10001: Code Injection Vulnerability in GitHub Enterprise Server Allows Arbitrary Code Execution via Message Handling

Vairav Advisory Report

Date: 2025-01-30

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A vulnerability CVE-2024-10001 has been identified in GitHub Enterprise Server. If exploited this vulnerability allows attackers to inject malicious code that will allow them to exfiltrate confidential data.

VULNERABILITY DETAILS

CVE-2024-10001

- **Description:** A code injection vulnerability was identified in GitHub Enterprise Server that allowed attackers to inject malicious code into the query selector via the identity property in the message handling function. This enabled the exfiltration of sensitive data by manipulating the DOM, including authentication tokens by dynamically embedding a hidden iframe on the page.
- **Impact:** If exploited, this vulnerability could impact the enterprise through regulatory fines and legal costs, loss of customer trust, operational disruptions and exposure of confidential data.
- **CVSS Score:** 7.1 (High)

AFFECTED VERSIONS

GitHub Enterprise Server versions before:

- 3.11.16
- 3.12.10
- 3.13.5
- 3.14.2
- 3.15.0

EXPLOIT DETAILS

This vulnerability could be exploited when the attacker is hosting a malicious website containing a hidden iframe and victim is logged into GitHub and interacts with the attacker controlled malicious webpage containing the iframe. Then, the attacker could use the hidden iframe to leak sensitive data from the DOM by injecting malicious input through the *identity* parameter in *querySelector* handling function which could lead to sensitive data exposure.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to the latest GitHub Enterprise Server versions:

- 3.11.16
- 3.12.10
- 3.13.5
- 3.14.2
- 3.15.0

ADDITIONAL SECURITY MEASURES

- Implement DLP (Data Loss Prevention) solutions to monitor data movement.
- Implement a strong Content Security Policy (CSP) and *SameSite* cookie attributes to prevent unauthorized iframes from interacting with GitHub Enterprise Server.
- Enforce strict access controls and harden GitHub Enterprise Server.
- Implement Input validation, parameterized queries and a Web Application Firewall (WAF) like ModSecurity.

REFERENCES

- https://app.opencve.io/cve/CVE-2024-10001
- https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.11
- https://vulners.com/cve/CVE-2024-10001

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com