CVE-2025-23369: GitHub Enterprise SAML Bypass FLAW

Vairav Advisory Report

Date: 2025-02-11

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability, CVE-2025-23369, has been identified in GitHub Enterprise Server that allows unauthorized internal users to spoof cryptographic signatures, potentially leading to unauthorized access and data compromise. If exploited, these vulnerabilities could lead to unauthorized access to GitHub Enterprise accounts, compromise of private repositories, and privilege escalation within an organization's GitHub environment.

VULNERABILITY DETAILS

CVE-2025-23369

- **Description:** An improper verification of cryptographic signatures in GitHub Enterprise Server allows unauthorized internal users to spoof signatures. This vulnerability stems from quirks in the libxml2 library used to parse SAML responses. By exploiting these quirks, an attacker can craft a malicious SAML response that bypasses authentication checks and gains access to arbitrary accounts.
- **Impact:** Exploitation of this vulnerability could lead to unauthorized access to GitHub Enterprise accounts, compromise of private repositories, and privilege escalation within an organization's GitHub environment.
- **CVSS Score:** 7.6 (High)

AFFECTED VERSIONS

GitHub Enterprise Server versions prior to:

- 3.12.14
- 3.13.10
- 3.14.7
- 3.15.2
- 3.16.0

EXPLOIT DETAILS

This vulnerability particularly concern environments where GitHub Enterprise Server is used with SAML single sign-on (SSO). Exploitation could lead to unauthorized access to GitHub Enterprise accounts, compromise of private repositories, and privilege escalation within an organization's GitHub environment. Instances not utilizing SAML SSO or where the attacker is not already an existing user are not impacted.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to the latest GitHub Enterprise Server versions for each affected version:

- 3.12.14
- 3.13.10
- 3.14.7
- 3.15.2
- 3.16.0

ADDITIONAL SECURITY MEASURES

- Restrict network access to the GitHub Enterprise Server to trusted IP addresses only.
- Disable unused authentication methods and enforce the use of strong, unique credentials for all users.
- Implement comprehensive logging of authentication attempts and regularly review logs for suspicious activities.
- Conduct periodic security assessments of your GitHub Enterprise Server configuration and apply recommended best practices.

REFERENCES

- GitHub Enterprise Server 3.12.14 Release Notes
- GitHub Enterprise Server 3.13.10 Release Notes
- GitHub Enterprise Server 3.14.7 Release Notes
- GitHub Enterprise Server 3.15.2 Release Notes
- NVD CVE-2025-23369 Details
- SecurityOnline.info Analysis and Exploit PoC

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