VULNERABILITIES IN GITHUB ENTERPRISE SERVER: RCE, XSS, AND INFORMATION DISCLOSURE RISKS

Vairav CVE Report

Date: April 21, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

GitHub has issued critical security updates for GitHub Enterprise Server to address multiple high-severity vulnerabilities, including a critical remote code execution flaw (CVE-2025-3509). The vulnerabilities impact versions 3.13.0 to 3.16.1 and could lead to full system compromise, unauthorized access to private repositories, and XSS attacks. Immediate patching is recommended.

VULNERABILITY DETAILS

CVE-2025-3509: Remote Code Execution via Pre-Receive Hooks

Description: A flaw in how GitHub Enterprise Server handles dynamically allocated ports during hot patch upgrades could allow attackers to execute arbitrary commands.

Impact: Full system takeover through remote code execution by privileged attackers.

CVSS Score: 7.1 (High)

Exploitation: Requires repository modification privileges or site administrator access during a specific hot patch window.

CVE-2025-3124: Unauthorized Access to Private Repository Names

Description: Improper authorization checks on the archived filter allow disclosure of private repository names in GitHub Advanced Security Overview.

Impact: Information disclosure that could aid attackers in targeting sensitive projects.

CVSS Score: 5.3 (Medium)

Exploitation: Exploitable through advanced search queries.

CVE-2025-3246: Cross-Site Scripting via Malicious Math Blocks

Description: Lack of sanitization in Markdown math blocks () allows attackers to inject malicious content.

Impact: Remote execution of HTML/CSS, leading to potential session hijacking or unauthorized actions.

CVSS Score: 8.6 (High)

Exploitation: Requires user interaction with the malicious Markdown content.

AFFECTED PRODUCTS/VERSIONS

- GitHub Enterprise Server 3.13.0–3.13.13 (fixed in 3.13.14)
- GitHub Enterprise Server 3.14.0–3.14.10 (fixed in 3.14.11)
- GitHub Enterprise Server 3.15.0–3.15.5 (fixed in 3.15.6)
- GitHub Enterprise Server 3.16.0–3.16.1 (fixed in 3.16.2)

RECOMMENDATIONS

- Upgrade immediately to patched versions: 3.13.14, 3.14.11, 3.15.6, or 3.16.2.
- Audit administrative and repository privileges regularly.
- Monitor hot patch activities for unusual access or behavior.
- Educate users on secure Markdown usage.
- Review logs and apply input sanitization where applicable.

Prompt updates and access control reviews are vital to mitigating the impact of these critical vulnerabilities.

REFERENCES

https://cybersecuritynews.com/github-enterprise-server-vulnerabilities/

https://www.cve.org/CVERecord?id=CVE-2025-3509

https://www.cve.org/CVERecord?id=CVE-2025-3124

https://www.cve.org/CVERecord?id=CVE-2025-3246

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: sales@vairavtech.com

Website: https://vairavtech.com