May 22, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware GitHub published a security advisory to address a critical vulnerability in the following products:

- GitHub Enterprise Server – versions 3.12.x prior to 3.12.4
- GitHub Enterprise Server – versions 3.11.x prior to 3.11.10
- GitHub Enterprise Server – versions 3.10.x prior to 3.10.12
- GitHub Enterprise Server – versions 3.9.x prior to 3.9.15

Technical Details

CRITICAL: On instances that use SAML single sign-on (SSO) authentication with the optional encrypted assertions feature, an attacker could forge a SAML response to provision and/or gain access to a user with administrator privileges.

Please note that encrypted assertions are not enabled by default. Instances not utilizing SAML SSO or utilizing SAML SSO authentication without encrypted assertions are not impacted. Exploitation of this vulnerability would allow unauthorized access to the instance without requiring prior authentication. GitHub has requested CVE ID CVE-2024-4985 for this vulnerability, which was reported via the GitHub Bug Bounty program.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-4985 CVE-2024-3646 CVE-2024-3684 CVE-2024-3470 CVE-2024-2440
- GitHub Release Notes #3.12.4
- GitHub Release Notes #3.11.10
- GitHub Release Notes #3.10.12
- GitHub Release Notes #3.9.15