August 21, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

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

- GitHub Enterprise Server – versions 3.13.x prior to 3.13.3
- GitHub Enterprise Server – versions 3.12.x prior to 3.12.8
- GitHub Enterprise Server – versions 3.11.x prior to 3.11.14
- GitHub Enterprise Server – versions 3.10.x prior to 3.10.16

Technical Details

CRITICAL: On GitHub Enterprise Server instances that use SAML single sign-on (SSO) authentication with specific IdPs utilizing publicly exposed signed federation metadata XML, an attacker could forge a SAML response to provision and/or gain access to a user account with site administrator privileges. GitHub has requested CVE ID CVE-2024-6800 for this vulnerability, which was reported via the GitHub Bug Bounty program.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist 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 at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-6800 , CVE-2024-7711, CVE-2024-6337
- GitHub Release Notes #3.13.3
- GitHub Release Notes #3.12.8
- GitHub Release Notes #3.11.14
- GitHub Release Notes #3.10.16