CERT-EU

Security Advisory 2024-047

Critical Vulnerability in GitHub Enterprise Server

May 22, 2024 — v1.0

TLP:CLEAR

History:

- *22/05/2024 — v1.0 – Initial publication*

Summary

On May 21, 2024, GitHub disclosed a critical vulnerability in GitHub Enterprise Server (GHES) impacting instances using SAML single sign-on (SSO) with encrypted assertions. This vulnerability allows attackers to forge SAML responses, granting unauthorised administrative access without authentication. [1]

A proof of concept is publicly available. CERT-EU strongly recommends updating as soon as possible. [2]

Technical Details

The vulnerability `CVE-2024-4985`, with a CVSS score of 10, involves SAML SSO with the optional encrypted assertions feature. An attacker could forge a SAML claim that contains correct user information. When GHES processes a fake SAML claim, it will not be able to validate its signature correctly, allowing an attacker to gain access to the GHES instance.

Affected Products

The following GitHub Enterprise Server versions are affected:

- 3.12.0 to 3.12.3;
- 3.11.0 to 3.11.9;
- 3.10.0 to 3.10.11;
- 3.9.0 to 3.9.14.

Only instances using SAML single sign-on (SSO) authentication are affected.

Recommendations

CERT-EU strongly recommends updating as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/github-warns-of-saml-auth-bypass-flaw-in-enterprise-server/

[2] https://github.com/absholi7ly/Bypass-authentication-GitHub-Enterprise-Server