مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in GitHub Enterprise Server

Tracking #:432316389

Date:14-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability, tracked as CVE-2024-9487, has been identified in GitHub Enterprise Server (GHES) that could lead to unauthorized user provisioning and access to the instance.

TECHNICAL DETAILS:

CVE-2024-9487,is a critical vulnerability affecting GitHub Enterprise Server, specifically related to improper verification of cryptographic signatures in the SAML SSO authentication mechanism. This flaw allows attackers to bypass SAML SSO authentication, potentially leading to unauthorized user provisioning and access to the instance.

Critical Severity Vulnerability:

- CVE ID: CVE-2024-9487
- Severity: Critical (CVSS 9.5)
- Exploitation required the encrypted assertions feature to be enabled, and the attacker would require direct network access as well as a signed SAML response or metadata document
- Affected Versions: All versions of GitHub Enterprise Server prior to 3.15
- Fixed Versions: 3.11.16, 3.12.10, 3.13.5, and 3.14.2.

RECOMMENDATIONS:

- Upgrade GitHub Enterprise Server to Fixed Versions as soon as possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-9487