مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Critical Vulnerability GitHub Enterprise Server (GHES)

Tracking #:432315879
Date:22-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in GitHub Enterprise Server (GHES) that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-4985**
- **CVSSv4 score: 10.0 Critical**
- An authentication bypass vulnerability exists in GitHub Enterprise Server (GHES) when using SAML single sign-on (SSO) authentication with the optional encrypted assertions feature. This vulnerability allowed an attacker to forge a SAML response to provision a new user account with site administrator privileges or gain access to an existing account with such privileges. Exploitation of this vulnerability would grant unauthorized access to the GHES instance.
- An attacker could exploit this vulnerability to gain full administrative control over a vulnerable GHES instance. This would allow them to access all data stored within the instance and perform any action on the system.

Affected Versions:

- GitHub Enterprise Server versions before 3.13.0

Fixed Versions:

- GitHub Enterprise Server versions 3.9.15, 3.10.12, 3.11.10 and 3.12.4.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the latest fixed version released by GitHub.

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-2024-4985
- https://docs.github.com/en/enterprise-server@3.12/admin/release-notes