مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authentication Bypass Vulnerabilities in ruby-saml

Tracking #:432318112

Date:09-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a two critical vulnerabilities have been identified in the ruby-saml library, enabling threat actors to bypass SAML assertion validation and impersonate users without legitimate credentials.

TECHNICAL DETAILS:

Two newly disclosed Critical (CVSS 9.3) vulnerabilities in the ruby-saml library—CVE-2025-66567 and CVE-2025-66568—allow threat actors to bypass SAML assertion validation and impersonate users without valid credentials. The flaws stem from XML parsing inconsistencies and canonicalization failures, enabling Signature Wrapping attacks, digest bypass, and signature replay.

Vulnerability Details

1. CVE-2025-66567 — Parser Differential Authentication Bypass

- Severity: Critical,9.3
- Affected Versions: < 1.18.0
- Patched Version: 1.18.0+
- The vulnerability does not affect the version 1.18.0.

2. CVE-2025-66568 — Canonicalization Error Leading to Digest/Signature Bypass

- Severity: Critical, ,9.3
- Affected Versions: < 1.18.0
- Patched Version: 1.18.0+
- The vulnerability does not affect the version 1.18.0.

RECOMMENDATIONS:

- Organizations are urged to update immediately to prevent authentication compromise across any SAML-integrated application.

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://github.com/advisories/GHSA-x4h9-gwv3-r4m4
- https://github.com/SAML-Toolkits/ruby-saml/security/advisories/GHSA-9v8j-x534-2fx3