مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Authentication Bypass Vulnerability in Node-SAML

Tracking #:432317546

Date:28-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Node-SAML that could potentially be exploited to bypass authentication controls in affected systems.

TECHNICAL DETAILS:

A critical vulnerability exists in **Node-SAML**, a widely used open-source library that enables **SAML 2.0** authentication in Node.js applications. Tracked as **CVE-2025-54369**, this flaw undermines the trust model of SAML authentication and exposes millions of users to risk, including **privilege escalation**, **account confusion**, and **SSO bypasses**.

Vulnerability Details:

- **CVE-2025-54369**
- CVSS Score 9.3 Critical
- The issue stems from how Node-SAML **processes SAML responses**. While the library **correctly verifies XML signatures**, it subsequently **parses the assertion data from the original, unsigned document** instead of the validated content.
- Node-SAML loads the assertion from the (unsigned) original response document. This is different than the parts that are verified when checking signature.
- This **discrepancy opens the door for attackers** to alter critical authentication data—such as usernames—in the SAML assertion **after the signature has been verified**, bypassing standard authentication controls.
- **Exploitation of this vulnerability can lead to:**
    - **Privilege Escalation:** Impersonate admin or privileged accounts
    - **Account Confusion:** Misroute users or trigger policy mismatches
    - **SSO Bypass:** Circumvent checks by the Identity Provider (IdP)

Affected Versions:

- All versions of Node-SAML prior to 5.1.0

Fixed Versions:

- Node-SAML 5.1.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Node-SAML.

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/node-saml/node-saml/security/advisories/GHSA-m837-g268-mmv7