مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SAML Signature Wrapping Vulnerability in samlify

Tracking #:432317288

Date:20-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed A critical SAML Signature Wrapping vulnerability in the samlify Node.js library. This flaw enables a SAML Signature Wrapping (SSW) attack, allowing attackers to bypass authentication and impersonate any user.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-47949**
- CVSSv4 Score: 9.9 (Critical)
- Vulnerability Type: SAML Signature Wrapping (SSW) / Improper Signature Validation
- A critical security vulnerability exists in the samlify Node.js library, which is widely used for implementing SAML 2.0-based Single Sign-On (SSO). This flaw allows attackers to exploit a SAML Signature Wrapping (SSW) weakness, enabling them to bypass authentication and impersonate any user, including privileged accounts.
- The vulnerability arises from inadequate validation of signed XML documents in SAML responses. An attacker can inject an unsigned, malicious assertion alongside a valid signed assertion. If the application processes the unsigned assertion, authentication controls are bypassed, enabling full user impersonation.
- Exploitation of this vulnerably can lead to:
    - Authentication Bypass: Attackers can authenticate as any user, including administrators.
    - Privilege Escalation: Potential for attackers to gain elevated access.
    - Unauthorized Access: Access to sensitive systems and data.
    - Lateral Movement: Attackers may move within compromised environments.

Affected Versions:

- samlify versions prior to v2.10.0

Fixed Versions:

- samlify v2.10.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by samlify.

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-2025-47949