مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Sentry's SAML SSO

Tracking #:432316768

Date:21-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Sentry's SAML SSO implementation, allowing attackers to take over any user account on a shared Sentry instance.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-22146) has been discovered in Sentry's SAML SSO implementation, allowing attackers to take over any user account on a shared Sentry instance.

Vulnerability Overview:

- CVE ID: CVE-2025-22146
- CVSS Base Score: 9.1 (Critical)
- Affected Product: Sentry (versions up to 25.0.x)
- Vulnerability Type: Improper Authentication (CWE-287)
- The vulnerability in Sentry's SAML SSO implementation allows an attacker to impersonate any user on a shared Sentry instance. The attack vector is network-based, requires no user interaction, and has low attack complexity.
- Exploitation involves:
  - Using a malicious SAML Identity Provider
  - Targeting another organization on the same Sentry instance
  - Knowing the victim's email address

Fixed Version:

- Users of self-hosted Sentry instances are advised to update immediately to version 25.1.0 or later to protect their systems. Sentry SaaS users have already been patched, with the fix deployed on January 14, 2025.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update sentry to the latest version.

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/getsentry/sentry/releases/tag/25.1.0