مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical XSS Vulnerability in Nagios XI

Tracking #:432317650
Date:28-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Nagios has addressed a significant cross-site scripting (XSS) vulnerability in Nagios XI that could allow remote attackers to execute arbitrary JavaScript code in users' browsers.

TECHNICAL DETAILS:

A critical Cross-Site Scripting (XSS) vulnerability exists in the Graph Explorer feature of Nagios XI. The flaw allows remote attackers to inject and execute arbitrary JavaScript code in the context of authenticated user sessions.

Given that Nagios XI is widely deployed for monitoring critical enterprise infrastructure, successful exploitation could compromise privileged administrator sessions, leading to severe security impacts.

Vulnerability Details:

- The XSS issue arises from insufficient input validation and output encoding in certain parameters within the Graph Explorer functionality. An attacker could craft malicious URLs or form submissions containing JavaScript payloads, which would execute in the context of a legitimate user session.
- Potential impacts include:
  - Theft of authentication cookies and session hijacking.
  - Unauthorized actions performed under the privileges of authenticated administrators.
  - Redirection of users to malicious websites.

Affected Product:

- Nagios XI

Fixed Versions

- 2024R2.1

RECOMMENDATIONS:

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

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://www.nagios.com/changelog/