مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Nagios XI

Tracking #:432318173

Date:24-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Nagios XI that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Nagios has released Nagios XI version 2026R1.1 to address a high-severity local privilege escalation vulnerability affecting earlier versions of the platform. The flaw could allow a local attacker to execute arbitrary code with root privileges, leading to full system compromise.

Vulnerability Details

- **CVE-2025-34288**
- **CVSS Score:** 8.6 High
- **CWE:** CWE-732 – Incorrect Permission Assignment for Critical Resource
- The vulnerability arises from an unsafe interaction between sudo permissions and file permissions within Nagios XI. A maintenance script that can be executed as root via sudo references an application file that is writable by lower-privileged users. This misconfiguration enables attackers to modify the file and inject malicious code.

Impact

An attacker with access to the Nagios application account can exploit this flaw by modifying the writable file. When a privileged user executes the affected maintenance script using sudo, the injected code runs with root-level privileges, bypassing standard privilege boundaries. Successful exploitation results in complete system compromise.

Affected Systems

- Nagios XI versions prior to 2026R1.1

Fixed Version

- Nagios XI 2026R1.1 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions 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://github.com/advisories/GHSA-2488-c4gj-6g77