Alert Bulletin

Bulletin N.: 2023-02
Publication Date: 16/11/2023
Subject: Alert 2023-02 – Critical Vulnerabilities in Nagios Products
Traffic Light Protocol (TLP): Amber

There have been ***reported*** critical SQL Injection vulnerabilities affecting the Nagios XI network monitoring software, which could result in privilege escalation.

The list of vulnerabilities is described below:

- ***CVE-2023-40933***– SQL Injection in the ad banner configuration with High criticality with score 8.8, allows authenticated attackers with ad banner configuration privileges to execute arbitrary SQL commands via the ID parameter sent to the update_banner_message() function.
- ***CVE-2023-40934***– SQL Injection in host/service escalation in Core Configuration Manager (CCM) with High criticality with score 7.
- ***CVE-2023-40931***– SQL injection in banner that recognizes the Medium criticality endpoint with a score of 6.5. Allows authenticated attackers to execute arbitrary SQL commands via the ID parameter in the POST request to /nagiosxi/admin/banner_message-ajaxhelper.php.
- ***CVE-2023-40932***– Cross-Site Scripting in the custom logo component with Medium criticality with score 5.4. Allows authenticated attackers with access to the custom logo component to inject javascript or HTML of their choice via the alternate text field. This affects all pages containing the navigation bar, including the login page, meaning the attacker can steal plain text credentials.