Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Security Vulnerabilities Uncovered in Nagios XI

Date of Publication	Admiralty Code	TA Number
September 22, 2023	A1	TA2023383

Summary

Discovered On: August 4, 2023
Affected Product: Nagios XI network monitoring software
Impact: Several security vulnerabilities have been identified in Nagios XI, a network monitoring software, which could potentially lead to privilege escalation and information disclosure. These vulnerabilities are tracked as CVE-2023-40931, CVE-2023-40932, CVE-2023-40933, and CVE-2023-40934.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-40931	Nagios SQL Injection Vulnerability	Nagios XI	✗	✗	✓
CVE-2023-40932	Nagios Cross-Site Scripting Vulnerability	Nagios XI	✗	✗	✓
CVE-2023-40933	Nagios SQL Injection Vulnerability	Nagios XI	✗	✗	✓
CVE-2023-40934	Nagios SQL Injection Vulnerability	Nagios XI	✗	✗	✓

Vulnerability Details

#1 Multiple security vulnerabilities have been disclosed in Nagios XI, a network monitoring software. These vulnerabilities could potentially lead to privilege escalation and information disclosure. They are tracked as CVE-2023-40931, CVE-2023-40932, CVE-2023-40933, and CVE-2023-40934. The security vulnerabilities in Nagios XI impact versions 5.11.1 and lower.

#2 The CVE-2023-40931 vulnerability is a SQL Injection vulnerability that affects the Banner acknowledging endpoint. It enables authenticated attackers to execute arbitrary SQL commands by manipulating the ID parameter within a POST request directed to '/nagiosxi/admin/banner_message-ajaxhelper.php'

#3 CVE-2023-40932 represents a Cross-Site Scripting (XSS) vulnerability that allows authenticated attackers with access to the custom logo component to inject arbitrary JavaScript or HTML code through the alt-text field. This vulnerability impacts all pages containing the navbar, including the login page, enabling attackers to potentially steal plaintext credentials.

#4 The CVE-2023-40933 vulnerability is an SQL Injection flaw associated with Announcement Banner Settings. An attacker can exploit this vulnerability by manipulating the query to execute arbitrary SQL commands against the application's database. To successfully exploit CVE-2023-40933, the attacker must possess certain privileges and be authenticated as an Administrator.

#5 CVE-2023-40934 is characterized by a SQL injection vulnerability that permits authenticated attackers, with the appropriate privileges for managing host escalations in the Core Configuration Manager, to execute arbitrary SQL commands. This security flaw arises when certain parameters, such as 'tfFirstNotif', 'tfLastNotif', and 'tfNotifInterval' are processed through a POST request.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-40931	Nagios XI versions 5.11.1 and lower	cpe:2.3:a:nagios:nagios_xi:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-40932	Nagios XI versions 5.11.1 and lower	cpe:2.3:a:nagios:nagios_xi:*:*:*:*:*:*:*:*	CWE-79
CVE-2023-40933	Nagios XI versions 5.11.1 and lower	cpe:2.3:a:nagios:nagios_xi:*:*:*:*:*:*:*:*	CWE-89
CVE-2023-40934	Nagios XI versions 5.11.1 and lower	cpe:2.3:a:nagios:nagios_xi:*:*:*:*:*:*:*:*	CWE-89

Recommendations

Apply Patch: Install the security patch provided by Nagios to address the CVE-2023-40931, CVE-2023-40932, CVE-2023-40933, and CVE-2023-40934 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Implement Web Application Firewall (WAF): Deploy a Web Application Firewall to protect against these vulnerabilities. The WAF can inspect and filter incoming web traffic, adding an extra layer of defense against potential threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0004** Privilege Escalation	**TA0002** Execution	**T1588** Obtain Capabilities
T1189 Drive-by Compromise	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application	**T1078** Valid Accounts
T1059 Command and Scripting Interpreter	**T1059.007** JavaScript		

Patch Details

To patch the vulnerability in Nagios, it's strongly recommended to upgrade to the Nagios XI 5.11.2 or later version,

Link:
https://www.nagios.com/products/security/

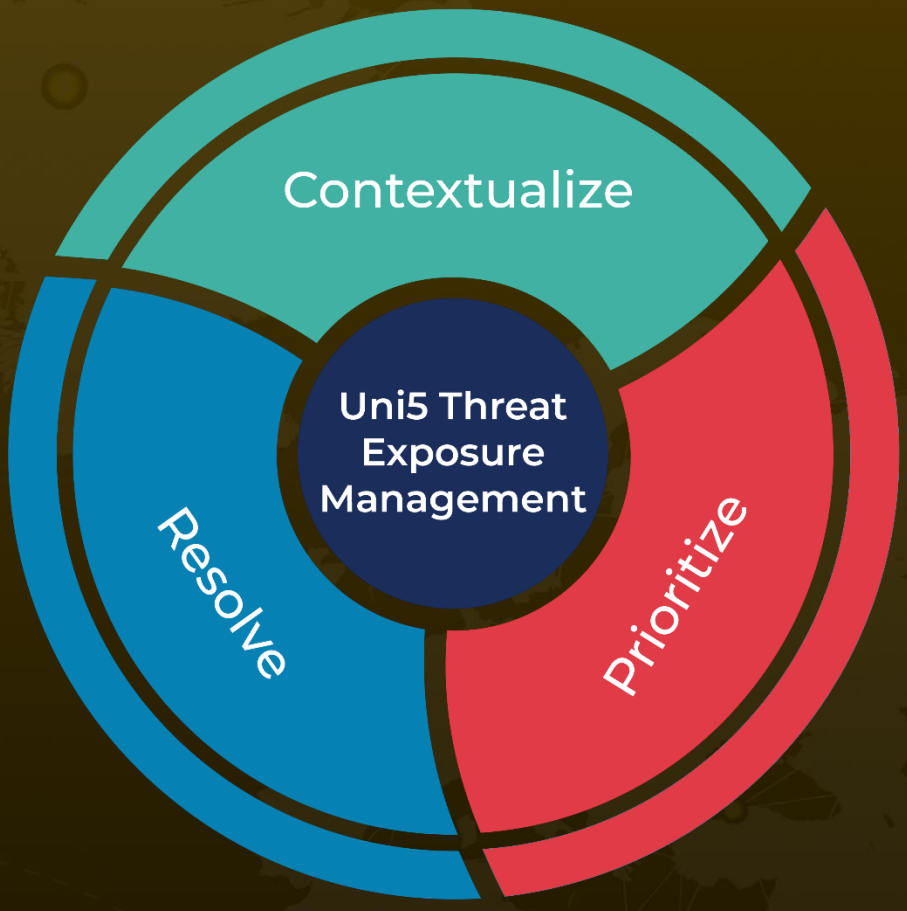
References

https://outpost24.com/blog/nagios-xi-vulnerabilities/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 22, 2023 . 6:00 AM

More at www.hivepro.com