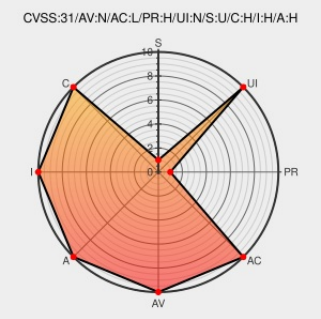
CVE-2020-5791

Published on: 10/20/2020 12:00:00 AM UTC

Last Modified on: 01/24/2023 04:10:00 PM UTC

CVE-2020-5791

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nagios Xi from Nagios contain the following vulnerability:

Improper neutralization of special elements used in an OS command in Nagios XI 5.7.3 allows a remote, authenticated admin user to execute operating system commands with the privileges of the apache user.

CVE-2020-5791 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Nagios XI 5.7.3 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162235/Nagios-XI-5.7.3-Remote-Code-Execution.html
Nagios XI Multiple Vulnerabilities - Research Advisory | Tenable®	Exploit Third Party Advisory	MISC www.tenable.com/security/research/tra-2020-58

	www.tenable.com text/html	
Nagios XI 5.7.3 Remote Command Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159743/Nagios-XI-5.7.3-Remote-Command-Injection.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nagios	Nagios Xi	5.7.3	All	All	All
Application	Nagios	Nagios Xi	5.7.3	All	All	All
Application	Nagios	Nagios Xi	All	All	All	All

cpe:2.3:a:nagios:nagios_xi:5.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:nagios:nagios_xi:5.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:nagios:nagios_xi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@amr00t	smiled: GET /cve/CVE-2020-5791 => generated 13374 bytes in 316 msecs	2021-06-01 03:51:40
@RemotelyAlerts	Severity: ??? | Improper neutralization of special eleme... | CVE-2020-5791 | Link for more: alerts.remotelyrmm.com/CVE-2020-5791	2022-06-15 04:28:25
@LinInfoSec	Nagios - CVE-2020-5791: tenable.com/security/resea…	2022-06-15 07:00:21

← Previous ID

Next ID→