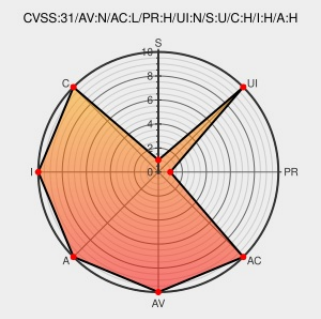
CVE-2020-35578

Published on: 01/13/2021 12:00:00 AM UTC

Last Modified on: 04/26/2021 05:34:00 PM UTC

CVE-2020-35578

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



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

An issue was discovered in the Manage Plugins page in Nagios XI before 5.8.0. Because the line-ending conversion feature is mishandled during a plugin upload, a remote, authenticated admin user can execute operating-system commands.

CVE-2020-35578 has been assigned by cve@mitre.org 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
Security Disclosures - Nagios	Vendor Advisory, www.nagios.com, text/html	CONFIRM www.nagios.com/products/security/
Nagios XI 5.7.x Remote Code Execution ≈	Exploit	MISC packetstormsecurity.com/files/160948/Nagios-XI-5.7.x-

Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	Remote-Code-Execution.html
Nagios XI Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162207/Nagios-XI-Remote-Code-Execution.html
Nagios XI Change Log - Nagios	Release Notes Vendor Advisory www.nagios.com text/html	MISC www.nagios.com/downloads/nagios-xi/change-log/

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	All	All	All	All
Application	Nagios	Nagios Xi	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CyberSecDN	#0daytoday #Nagios XI 5.8.0 Remote Code Execution #Exploit #RCE #CVE-2020-35578 0day.today/exploit/descri… via @inj3ct0r	2021-05-08 03:47:17
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-35578.… twitter.com/i/web/status/1…	2021-05-10 05:02:01
@ipssignatures	I know one more IPS that has a protection/signature/rule for the vulnerability CVE-2020-35578. ipssignatures.appspot.com/?cve=CVE-2020-… #Sdklei6la43pxa	2021-05-10 05:02:01
@ipssignatures	It's new to me that WatchGuard has a protection/signature/rule for the vulnerability CVE-2020-35578. … twitter.com/i/web/status/1…	2021-05-11 19:02:00
@ipssignatures	I know 2 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-35578. ipssignatures.appspot.com/?cve=CVE-2020-… #Sdklei6la43pxa	2021-05-11 19:02:01
@pwnwikiorg	CVE-2020-35578 Nagios XI 遠程命令執行漏洞 pwnwiki.org/index.php?titl…	2021-05-30 02:21:08
@ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2020-35578.… twitter.com/i/web/status/1…	2021-07-28 03:02:01
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-35578. ipssignatures.appspot.com/?cve=CVE-2020-… #Sdklei6la43pxa	2021-07-28 03:02:01

← Previous ID

Next ID→