



# 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 [M](#) 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>HIGH</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                             | Tags                                                                                           | Link                                                                       |
|-----------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Security Disclosures - Nagios           | <a href="#">Vendor Advisory</a><br><a href="#">www.nagios.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM www.nagios.com/products/security/</a>                  |
| Nagios XI 5.7.x Remote Code Execution ≈ | <a href="#">Exploit</a>                                                                        | <a href="#">MISC packetstormsecurity.com/files/160948/Nagios-XI-5.7.x-</a> |

|                                                |                                                                                                                                           |                                                                                                                                                                                  |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Packet Storm                                   | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a> | <a href="#">Remote-Code-Execution.html</a>                                                                                                                                       |
| Nagios XI Remote Code Execution ≈ Packet Storm | <a href="#">packetstormsecurity.com</a><br><a href="#">text/html</a>                                                                      |  <a href="#">MISC packetstormsecurity.com/files/162207/Nagios-XI-Remote-Code-Execution.html</a> |
| Nagios XI Change Log - Nagios                  | <a href="#">Release Notes</a><br><a href="#">Vendor Advisory</a><br><a href="#">www.nagios.com</a><br><a href="#">text/html</a>           |  <a href="#">MISC www.nagios.com/downloads/nagios-xi/change-log/</a>                            |

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

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)