

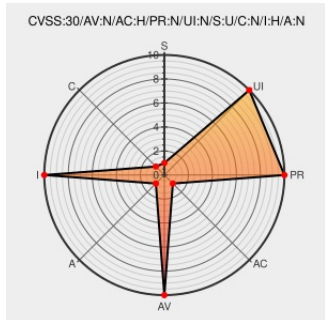


# CVE-2016-5117

Published on: 01/31/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

## CVE-2016-5117

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openntpd](#) from [Openntpd](#) contain the following vulnerability:

OpenNTPD before 6.0p1 does not validate the CN for HTTPS constraint requests, which allows remote attackers to bypass the man-in-the-middle mitigations via a crafted timestamp constraint with a valid certificate.

CVE-2016-5117 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                                                            | Tags                                                                                                                                  | Link                                                                                                                  |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| oss-security - CVE request: OpenNTPD not verifying CN during HTTPS constraints request | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">www.openwall.com</a><br><a href="#">text/html</a> | <a href="#">MLIST [oss-security] 20160523 CVE request: OpenNTPD not verifying CN during HTTPS constraints request</a> |

oss-security - Re: CVE request: OpenNTPD not verifying CN during HTTPS constraints request

Mailing List

Third Party Advisory

www.openwall.com

text/html

MLIST [oss-security] 20160529 Re: CVE request: OpenNTPD not verifying CN during HTTPS constraints request

Vendor Advisory

www.openntpd.org

text/plain

CONFIRM

www.openntpd.org/txt/release-6.0p1.txt

Patch

cvsweb.openbsd.org

text/x-diff

CONFIRM

cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.sbin/ntpd/constraint.c.diff?r1=1.27&r2=1.28

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                        | <a href="#">Openntpd</a> | <a href="#">Openntpd</a> | All     | All    | All     | All      |
| cpe:2.3:a:openntpd:openntpd:*****: |                          |                          |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →