



CVE-2017-11506

Published on: 08/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

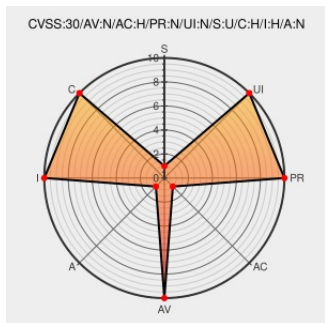
CVE-2017-11506

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Nessus** from **Tenable** contain the following vulnerability:

When linking a Nessus scanner or agent to Tenable.io or other manager, Nessus 6.x before 6.11 does not verify the manager's TLS certificate when making the initial outgoing connection. This could allow man-in-the-middle attacks.

CVE-2017-11506 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Tenable - Nessus** version **6.x before 6.11**

CVSS3 Score: **7.4 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Tenable Nessus TLS Certificate Validation Flaw Lets Certain Remote Users Access and Modify Data Communicated Between a Scanner and a Manager - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTrack 1039141

Security Headers

www.securitytrackers.com

text/html

[R1] Nessus 6.11 Fixes One Vulnerability - Security Advisory | Tenable™

Vendor Advisory

www.tenable.com

text/html

 CONFIRM

www.tenable.com/security/tns-2017-11

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	Tenable	Nessus	6.0.0	All	All	All
Application	Tenable	Nessus	6.0.1	All	All	All
Application	Tenable	Nessus	6.0.2	All	All	All
Application	Tenable	Nessus	6.1.0	All	All	All
Application	Tenable	Nessus	6.1.1	All	All	All
Application	Tenable	Nessus	6.1.2	All	All	All
Application	Tenable	Nessus	6.10.0	All	All	All
Application	Tenable	Nessus	6.10.1	All	All	All
Application	Tenable	Nessus	6.10.2	All	All	All
Application	Tenable	Nessus	6.10.3	All	All	All
Application	Tenable	Nessus	6.10.4	All	All	All
Application	Tenable	Nessus	6.10.5	All	All	All
Application	Tenable	Nessus	6.10.6	All	All	All
Application	Tenable	Nessus	6.10.7	All	All	All
Application	Tenable	Nessus	6.10.8	All	All	All
Application	Tenable	Nessus	6.10.9	All	All	All
Application	Tenable	Nessus	6.2.0	All	All	All
Application	Tenable	Nessus	6.2.1	All	All	All
Application	Tenable	Nessus	6.3.0	All	All	All
Application	Tenable	Nessus	6.3.1	All	All	All
Application	Tenable	Nessus	6.3.2	All	All	All
Application	Tenable	Nessus	6.3.3	All	All	All
Application	Tenable	Nessus	6.3.4	All	All	All
Application	Tenable	Nessus	6.3.5	All	All	All
Application	Tenable	Nessus	6.3.6	All	All	All

Application	Tenable	Nessus	6.3.6	All	All	All
Application	Tenable	Nessus	6.3.7	All	All	All
Application	Tenable	Nessus	6.4.0	All	All	All
Application	Tenable	Nessus	6.4.1	All	All	All
Application	Tenable	Nessus	6.4.2	All	All	All
Application	Tenable	Nessus	6.4.3	All	All	All
Application	Tenable	Nessus	6.5.0	All	All	All
Application	Tenable	Nessus	6.5.1	All	All	All
Application	Tenable	Nessus	6.5.2	All	All	All
Application	Tenable	Nessus	6.5.3	All	All	All
Application	Tenable	Nessus	6.5.4	All	All	All
Application	Tenable	Nessus	6.5.5	All	All	All
Application	Tenable	Nessus	6.5.6	All	All	All
Application	Tenable	Nessus	6.6.0	All	All	All
Application	Tenable	Nessus	6.6.1	All	All	All
Application	Tenable	Nessus	6.6.2	All	All	All
Application	Tenable	Nessus	6.7.0	All	All	All
Application	Tenable	Nessus	6.8.0	All	All	All
Application	Tenable	Nessus	6.8.1	All	All	All
Application	Tenable	Nessus	6.9.0	All	All	All
Application	Tenable	Nessus	6.9.1	All	All	All
Application	Tenable	Nessus	6.9.2	All	All	All
Application	Tenable	Nessus	6.9.3	All	All	All
Application	Tenable	Nessus	6.0.0	All	All	All
Application	Tenable	Nessus	6.0.1	All	All	All
Application	Tenable	Nessus	6.0.2	All	All	All
Application	Tenable	Nessus	6.1.0	All	All	All
Application	Tenable	Nessus	6.1.1	All	All	All
Application	Tenable	Nessus	6.1.2	All	All	All
Application	Tenable	Nessus	6.10.0	All	All	All
Application	Tenable	Nessus	6.10.1	All	All	All
Application	Tenable	Nessus	6.10.2	All	All	All
Application	Tenable	Nessus	6.10.3	All	All	All
Application	Tenable	Nessus	6.10.4	All	All	All
Application	Tenable	Nessus	6.10.5	All	All	All
Application	Tenable	Nessus	6.10.6	All	All	All

Application	Tenable	Nessus	6.10.7	All	All	All
Application	Tenable	Nessus	6.10.8	All	All	All
Application	Tenable	Nessus	6.10.9	All	All	All
Application	Tenable	Nessus	6.2.0	All	All	All
Application	Tenable	Nessus	6.2.1	All	All	All
Application	Tenable	Nessus	6.3.0	All	All	All
Application	Tenable	Nessus	6.3.1	All	All	All
Application	Tenable	Nessus	6.3.2	All	All	All
Application	Tenable	Nessus	6.3.3	All	All	All
Application	Tenable	Nessus	6.3.4	All	All	All
Application	Tenable	Nessus	6.3.5	All	All	All
Application	Tenable	Nessus	6.3.6	All	All	All
Application	Tenable	Nessus	6.3.7	All	All	All
Application	Tenable	Nessus	6.4.0	All	All	All
Application	Tenable	Nessus	6.4.1	All	All	All
Application	Tenable	Nessus	6.4.2	All	All	All
Application	Tenable	Nessus	6.4.3	All	All	All
Application	Tenable	Nessus	6.5.0	All	All	All
Application	Tenable	Nessus	6.5.1	All	All	All
Application	Tenable	Nessus	6.5.2	All	All	All
Application	Tenable	Nessus	6.5.3	All	All	All
Application	Tenable	Nessus	6.5.4	All	All	All
Application	Tenable	Nessus	6.5.5	All	All	All
Application	Tenable	Nessus	6.5.6	All	All	All
Application	Tenable	Nessus	6.6.0	All	All	All
Application	Tenable	Nessus	6.6.1	All	All	All
Application	Tenable	Nessus	6.6.2	All	All	All
Application	Tenable	Nessus	6.7.0	All	All	All
Application	Tenable	Nessus	6.8.0	All	All	All
Application	Tenable	Nessus	6.8.1	All	All	All
Application	Tenable	Nessus	6.9.0	All	All	All
Application	Tenable	Nessus	6.9.1	All	All	All
Application	Tenable	Nessus	6.9.2	All	All	All
Application	Tenable	Nessus	6.9.3	All	All	All

```
cpe:2.3:a:tenable:nessus:6.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.2.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.2.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.3.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.4.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.4.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.4.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.4.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.4:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.5.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.6.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.6.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.6.2:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.7.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.8.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.8.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.9.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.9.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.9.2:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.9.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.0.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.1.1:*.*.*.*.*.*.*.*.:
```

```
cpe:2.3:a:tenable:nessus:6.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.0:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.1:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.2:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.3:*:*:*:*:*:
```

```
cpe:2.3:a:tenable:nessus:6.10.4:*:*:*:*:*:*:
```

cpe:2.3:a:tenable:nessus:6.10.5:*****:
cpe:2.3:a:tenable:nessus:6.10.6:*****:
cpe:2.3:a:tenable:nessus:6.10.7:*****:
cpe:2.3:a:tenable:nessus:6.10.8:*****:
cpe:2.3:a:tenable:nessus:6.10.9:*****:
cpe:2.3:a:tenable:nessus:6.2.0:*****:
cpe:2.3:a:tenable:nessus:6.2.1:*****:
cpe:2.3:a:tenable:nessus:6.3.0:*****:
cpe:2.3:a:tenable:nessus:6.3.1:*****:
cpe:2.3:a:tenable:nessus:6.3.2:*****:
cpe:2.3:a:tenable:nessus:6.3.3:*****:
cpe:2.3:a:tenable:nessus:6.3.4:*****:
cpe:2.3:a:tenable:nessus:6.3.5:*****:
cpe:2.3:a:tenable:nessus:6.3.6:*****:
cpe:2.3:a:tenable:nessus:6.3.7:*****:
cpe:2.3:a:tenable:nessus:6.4.0:*****:
cpe:2.3:a:tenable:nessus:6.4.1:*****:
cpe:2.3:a:tenable:nessus:6.4.2:*****:
cpe:2.3:a:tenable:nessus:6.4.3:*****:
cpe:2.3:a:tenable:nessus:6.5.0:*****:
cpe:2.3:a:tenable:nessus:6.5.1:*****:
cpe:2.3:a:tenable:nessus:6.5.2:*****:
cpe:2.3:a:tenable:nessus:6.5.3:*****:
cpe:2.3:a:tenable:nessus:6.5.4:*****:
cpe:2.3:a:tenable:nessus:6.5.5:*****:
cpe:2.3:a:tenable:nessus:6.5.6:*****:
cpe:2.3:a:tenable:nessus:6.6.0:*****:
cpe:2.3:a:tenable:nessus:6.6.1:*****:

cpe:2.3:a:tenable:nessus:6.6.2:*****:
cpe:2.3:a:tenable:nessus:6.7.0:*****:
cpe:2.3:a:tenable:nessus:6.8.0:*****:
cpe:2.3:a:tenable:nessus:6.8.1:*****:
cpe:2.3:a:tenable:nessus:6.9.0:*****:
cpe:2.3:a:tenable:nessus:6.9.1:*****:
cpe:2.3:a:tenable:nessus:6.9.2:*****:
cpe:2.3:a:tenable:nessus:6.9.3:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →