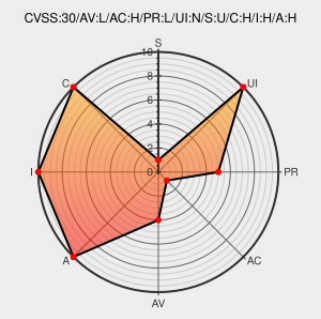
CVE-2018-1141

Published on: 03/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:32 PM UTC

CVE-2018-1141

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



Certain versions of Nessus from Tenable contain the following vulnerability:

When installing Nessus to a directory outside of the default location, Nessus versions prior to 7.0.3 did not enforce secure permissions for sub-directories. This could allow for local privilege escalation if users had not secured the directories in the installation location.

CVE-2018-1141 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Tenable** - **Nessus** version **All versions prior to 7.0.3**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Tenable Nessus Permissions Error for Non-Default Directory Installation Lets Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com	SECTRACK 1040557

	text/html	
[R2] Nessus 7.0.3 Fixes One Vulnerability - Security Advisory | Tenable®	Vendor Advisory www.tenable.com text/html	CONFIRM www.tenable.com/security/tns-2018-01

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	All	All	All	All
Application	Tenable	Nessus	All	All	All	All

cpe:2.3:a:tenable:nessus:*:*:*:*:*:*:*:*:

cpe:2.3:a:tenable:nessus:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→