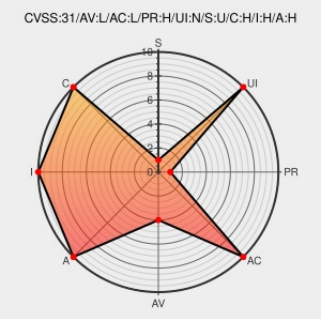
CVE-2021-20135

Published on: 11/02/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-20135

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



Certain versions of Nessus from Tenable contain the following vulnerability:

Nessus versions 8.15.2 and earlier were found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. Tenable has included a fix for this issue in Nessus 10.0.0. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/nessus).

CVE-2021-20135 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
[R1] Nessus 10.0.0 Fixes One Vulnerability - Security Advisory | Tenable®	www.tenable.com text/html	MISC www.tenable.com/security/tns-2021-18

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20135 : Nessus versions 8.15.2 and earlier were found to contain a local privilege escalation vulnerabilit… twitter.com/i/web/status/1…	2021-11-03 00:06:58

← Previous ID

Next ID→