



CVE-2021-20077

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-20077
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-19 19:15:00 UTC
Updated	2022-10-28 14:28:00 UTC
Description	Nessus Agent versions 7.2.0 through 8.2.2 were found to inadvertently capture the IAM role security token on the local host

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tenable	Nessus Agent	All	All	All	All
Application	Tenable	Nessus Agent	All	All	All	All
Application	Tenable	Nessus Agent	All	All	All	All

References

Reference	Source	Link	Tags
[R1] Nessus Agent 8.2.3 Fixes Multiple Vulnerabilities - Security Advisory Tenable®	MISC	www.tenable.com	
[R1] Nessus 8.14.0 Fixes One Vulnerability - Security Advisory Tenable®	CONFIRM	www.tenable.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)