



CVE-2023-0524

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-0524
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-01 03:15:00 UTC
Updated	2023-02-07 22:43:00 UTC
Description	As part of our Security Development Lifecycle, a potential privilege escalation issue was identified internally. This could allow

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	-	All	All	All
Application	Tenable	Tenable.io	-	All	All	All
Application	Tenable	Tenable.sc	-	All	All	All

References

Reference	Source	Link
[R1] Tenable Plugin Feed ID #202212212055 Fixes Privilege Escalation Vulnerability - Security Advisory Tenable®	MISC	www.tenable.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report