



CVE-2019-19747

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

Summary

CVE	CVE-2019-19747
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-20 17:15:00 UTC
Updated	2020-01-03 16:21:00 UTC
Description	NeuVector 3.1 when configured to allow authentication via Active Directory, does not enforce non-empty passwords which a

Risk And Classification

Problem Types: CWE-521

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Neuvector	Neuvector	All	All	All	All

References

Reference	Source	Link	Tags
Blog - NeuVector	MISC	neuvector.com	Vendor Advisory
CVE-2019-19747 Read	MISC	paulrobertson.co.za	Exploit, Third Party Advisory
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.

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