



CVE-2017-4920

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

Summary

CVE	CVE-2017-4920
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-05 21:29:00 UTC
Updated	2017-12-22 19:50:00 UTC
Description	The implementation of the OSPF protocol in VMware NSX-V Edge 6.2.x prior to 6.2.8 and NSX-V Edge 6.3.x prior to 6.3.3

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Nsx-v Edge	All	All	All	All
Application	Vmware	Nsx-v Edge	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2017-0014	CONFIRM	www.vmware.com	Vendor Advisory
Malformed Request	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
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.

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