



CVE-2019-16991

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

Summary

CVE	CVE-2019-16991
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-21 16:15:00 UTC
Updated	2023-02-03 21:29:00 UTC
Description	In FusionPBX up to v4.5.7, the file app\edit\filedelete.php uses an unsanitized "file" variable coming from the URL, which is

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
FusionPBX XSS 20 – Resp3ct blog	MISC	resp3ctblog.wordpress.com	Third Party Advisory
Update filedelete.php · fusionpbx/fusionpbx@cd4632b · GitHub	MISC	github.com	Patch
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