CVE-2016-3125

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2016-3125
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-05 20:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile di

Risk And Classification

Problem Types: CWE-310 | CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Application	Proftpd	Proftpd	1.3.6	rc1	All	All
Application	Proftpd	Proftpd	1.3.6	rc1	All	All
Application	Proftpd	Proftpd	All	a	All	All

References

Reference	Sc
oss-security - Re: ProFTPD before 1.3.5b/1.3.6rc2 uses 1024 bit Diffie Hellman parameters for TLS even if user sets manual parameters	MI
proftpd.org/docs/NEWS-1.3.5b	C(
proftpd.org/docs/NEWS-1.3.6rc2	C(
Bug 4230 – TLSDHParamFile directive appears ignored because unexpected DH is chosen	C(
[SECURITY] Fedora 23 Update: proftpd-1.3.5b-1.fc23	FE

oss-security - ProFTPD before 1.3.5b/1.3.6rc2 uses 1024 bit Diffie Hellman parameters for TLS even if user sets manual parameters	MI
[SECURITY] Fedora 22 Update: proftpd-1.3.5b-1.fc22	FE
openSUSE-SU-2016:1334-1: moderate: Security update for proftpd	SU
openSUSE-SU-2016:1558-1: moderate: Security update for proftpd	SU
[SECURITY] Fedora 24 Update: proftpd-1.3.5b-1.fc24	FE
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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