



CVE-2015-3306

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

Summary

CVE	CVE-2015-3306
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-18 15:59:00 UTC
Updated	2021-05-26 20:15:00 UTC
Description	The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Proftpd	Proftpd	1.3.5	All	All	All
Application	Proftpd	Proftpd	1.3.5	All	All	All

References

Reference	Source	Link	Tags
ProFTPD 1.3.5 Remote Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
ProFTPD CPFR / CPTO Proof Of Concept ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE-2015-3306 ProFTPD 1.3.5 Mod_Copy Command Execution Rapid7	MISC	www.rapid7.com	
ProFTPD 1.3.5 File Copy ≈ Packet Storm	MISC	packetstormsecurity.com	
Debian -- Security Information -- DSA-3263-1 proftpd-dfsg	DEBIAN	www.debian.org	
[SECURITY] Fedora 21 Update: proftpd-1.3.5-5.fc21	FEDORA	lists.fedoraproject.org	
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution - Linux remote Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit
[SECURITY] Fedora 20 Update: proftpd-1.3.4e-3.fc20	FEDORA	lists.fedoraproject.org	
openSUSE-SU-2015:1031-1: moderate: Security update for proftpd	SUSE	lists.opensuse.org	
ProFTPD 1.3.5 Mod_Copy Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] Fedora 22 Update: proftpd-1.3.5-6.fc22	FEDORA	lists.fedoraproject.org	
ProFTPD CVE-2015-3306 Information Disclosure Vulnerabilities	BID	www.securityfocus.com	

ProFTPD 1.3.5 - File Copy	EXPLOIT-DB	www.exploit-db.com	Exploit
ProFTPD 1.3.5 Remote Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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