



CVE-2010-3867

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

Summary

CVE	CVE-2010-3867
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-09 21:00:00 UTC
Updated	2011-09-15 03:17:00 UTC
Description	Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticate

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Proftpd	Proftpd	1.2.10	All	All	All
Application	Proftpd	Proftpd	1.2.10	rc1	All	All
Application	Proftpd	Proftpd	1.2.10	rc2	All	All
Application	Proftpd	Proftpd	1.2.10	rc3	All	All
Application	Proftpd	Proftpd	1.3.0	All	All	All
Application	Proftpd	Proftpd	1.3.0	a	All	All
Application	Proftpd	Proftpd	1.3.0	rc1	All	All
Application	Proftpd	Proftpd	1.3.0	rc2	All	All
Application	Proftpd	Proftpd	1.3.0	rc3	All	All
Application	Proftpd	Proftpd	1.3.0	rc4	All	All
Application	Proftpd	Proftpd	1.3.0	rc5	All	All
Application	Proftpd	Proftpd	1.3.1	All	All	All
Application	Proftpd	Proftpd	1.3.1	rc1	All	All
Application	Proftpd	Proftpd	1.3.1	rc2	All	All
Application	Proftpd	Proftpd	1.3.1	rc3	All	All
Application	Proftpd	Proftpd	1.3.2	All	All	All
Application	Proftpd	Proftpd	1.3.2	a	All	All

Application	Proftpd	Proftpd	1.3.2	b	All	All
Application	Proftpd	Proftpd	1.3.2	c	All	All
Application	Proftpd	Proftpd	1.3.2	d	All	All
Application	Proftpd	Proftpd	1.3.2	e	All	All
Application	Proftpd	Proftpd	1.3.2	rc1	All	All
Application	Proftpd	Proftpd	1.3.2	rc2	All	All
Application	Proftpd	Proftpd	1.3.2	rc3	All	All
Application	Proftpd	Proftpd	1.3.2	rc4	All	All
Application	Proftpd	Proftpd	1.3.3	All	All	All
Application	Proftpd	Proftpd	1.3.3	a	All	All
Application	Proftpd	Proftpd	1.3.3	b	All	All
Application	Proftpd	Proftpd	1.3.3	rc1	All	All
Application	Proftpd	Proftpd	1.3.3	rc2	All	All
Application	Proftpd	Proftpd	1.3.3	rc3	All	All
Application	Proftpd	Proftpd	1.3.3	rc4	All	All
Application	Proftpd	Proftpd	1.2.10	All	All	All
Application	Proftpd	Proftpd	1.2.10	rc1	All	All
Application	Proftpd	Proftpd	1.2.10	rc2	All	All
Application	Proftpd	Proftpd	1.2.10	rc3	All	All
Application	Proftpd	Proftpd	1.3.0	All	All	All
Application	Proftpd	Proftpd	1.3.0	a	All	All
Application	Proftpd	Proftpd	1.3.0	rc1	All	All
Application	Proftpd	Proftpd	1.3.0	rc2	All	All
Application	Proftpd	Proftpd	1.3.0	rc3	All	All
Application	Proftpd	Proftpd	1.3.0	rc4	All	All
Application	Proftpd	Proftpd	1.3.0	rc5	All	All
Application	Proftpd	Proftpd	1.3.1	All	All	All
Application	Proftpd	Proftpd	1.3.1	rc1	All	All
Application	Proftpd	Proftpd	1.3.1	rc2	All	All
Application	Proftpd	Proftpd	1.3.1	rc3	All	All
Application	Proftpd	Proftpd	1.3.2	All	All	All
Application	Proftpd	Proftpd	1.3.2	a	All	All
Application	Proftpd	Proftpd	1.3.2	b	All	All
Application	Proftpd	Proftpd	1.3.2	c	All	All
Application	Proftpd	Proftpd	1.3.2	d	All	All

Application	Proftpd	Proftpd	1.3.2	e	All	All
Application	Proftpd	Proftpd	1.3.2	rc1	All	All
Application	Proftpd	Proftpd	1.3.2	rc2	All	All
Application	Proftpd	Proftpd	1.3.2	rc3	All	All
Application	Proftpd	Proftpd	1.3.2	rc4	All	All
Application	Proftpd	Proftpd	1.3.3	All	All	All
Application	Proftpd	Proftpd	1.3.3	a	All	All
Application	Proftpd	Proftpd	1.3.3	b	All	All
Application	Proftpd	Proftpd	1.3.3	rc1	All	All
Application	Proftpd	Proftpd	1.3.3	rc2	All	All
Application	Proftpd	Proftpd	1.3.3	rc3	All	All
Application	Proftpd	Proftpd	1.3.3	rc4	All	All

References

Reference	Source	Link	Tags
Fedora update for proftpd - Secunia.com	SECUNIA	secunia.com	
[SECURITY] Fedora 12 Update: proftpd-1.3.3c-1.fc12	FEDORA	lists.fedoraproject.org	
Bug 3519 – Inappropriate directory traversal allowed by mod_site_misc	CONFIRM	bugs.proftpd.org	
Debian -- Security Information -- DSA-2191-1 proftpd-dfsg	DEBIAN	www.debian.org	
ProFTPD Multiple Remote Vulnerabilities	BID	www.securityfocus.com	Explo
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
Slackware update for proftpd - Advisories - Community	SECUNIA	secunia.com	
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	slackware.com	
[SECURITY] Fedora 14 Update: proftpd-1.3.3c-1.fc14	FEDORA	lists.fedoraproject.org	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
Support / Security / Advisories // MDVSA-2010:227 Mandriva	MANDRIVA	www.mandriva.com	
oss-security - Re: Proftpd pre-authentication buffer overflow in Telnet code	MLIST	www.openwall.com	
404 Not Found	CONFIRM	www.proftpd.org	
[SECURITY] Fedora 13 Update: proftpd-1.3.3c-1.fc13	FEDORA	lists.fedoraproject.org	
ProFTPD Directory Traversal and Buffer Overflow Vulnerabilities - Advisories - Community	SECUNIA	secunia.com	Vend
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)