



# CVE-2004-0432

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-0432
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-08-18 04:00:00 UTC
<b>Updated</b>	2017-07-11 01:30:00 UTC
<b>Description</b>	ProFTPD 1.2.9 treats the Allow and Deny directives for CIDR based ACL entries as if they were AllowAll, which could allow

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.5	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	0.7	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.1a	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.2	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc1	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc2	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	rc3	All	All
Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.9	All	All	All

Application	<a href="#">Proftpd Project</a>	<a href="#">Proftpd</a>	1.2.9	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All

## References

Reference	Source	Link	Ta
'TSLSA-2004-0025 - multi' - MARC	TRUSTIX	<a href="#">marc.info</a>	
Advisories - Mandriva	MANDRAKE	<a href="#">www.mandriva.com</a>	
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>	
ProFTPD CIDR Access Control Rule Bypass Vulnerability	BID	<a href="#">www.securityfocus.com</a>	Pe
Secunia - Advisories - ProFTPD CIDR Addressing ACL and "site chgrp" Security Issues	SECUNIA	<a href="#">secunia.com</a>	
Bug 2267 – Broken IP subnet matching	CONFIRM	<a href="#">bugs.proftpd.org</a>	
'[OpenPKG-SA-2004.018] OpenPKG Security Advisory (proftpd)' - MARC	BUGTRAQ	<a href="#">marc.info</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	ca

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](#)