



CVE-2004-2408

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

Summary

CVE	CVE-2004-2408
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	Linux VServer 1.27 and earlier, 1.3.9 and earlier, and 1.9.1 and earlier shares /proc permissions across all virtual and host

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vserver	Linux-vserver	1.20	All	All	All
Application	Vserver	Linux-vserver	1.21	All	All	All
Application	Vserver	Linux-vserver	1.22	All	All	All
Application	Vserver	Linux-vserver	1.23	All	All	All
Application	Vserver	Linux-vserver	1.24	All	All	All
Application	Vserver	Linux-vserver	1.25	All	All	All
Application	Vserver	Linux-vserver	1.26	All	All	All
Application	Vserver	Linux-vserver	1.27	All	All	All
Application	Vserver	Linux-vserver	1.3.0	All	All	All
Application	Vserver	Linux-vserver	1.3.1	All	All	All
Application	Vserver	Linux-vserver	1.3.2	All	All	All
Application	Vserver	Linux-vserver	1.3.3	All	All	All
Application	Vserver	Linux-vserver	1.3.4	All	All	All
Application	Vserver	Linux-vserver	1.3.5	All	All	All
Application	Vserver	Linux-vserver	1.3.6	All	All	All
Application	Vserver	Linux-vserver	1.3.7	All	All	All
Application	Vserver	Linux-vserver	1.3.8	All	All	All

Application	Vserver	Linux-vserver	1.3.9	All	All	All
Application	Vserver	Linux-vserver	1.9.1	All	All	All
Application	Vserver	Linux-vserver	1.20	All	All	All
Application	Vserver	Linux-vserver	1.21	All	All	All
Application	Vserver	Linux-vserver	1.22	All	All	All
Application	Vserver	Linux-vserver	1.23	All	All	All
Application	Vserver	Linux-vserver	1.24	All	All	All
Application	Vserver	Linux-vserver	1.25	All	All	All
Application	Vserver	Linux-vserver	1.26	All	All	All
Application	Vserver	Linux-vserver	1.27	All	All	All
Application	Vserver	Linux-vserver	1.3.0	All	All	All
Application	Vserver	Linux-vserver	1.3.1	All	All	All
Application	Vserver	Linux-vserver	1.3.2	All	All	All
Application	Vserver	Linux-vserver	1.3.3	All	All	All
Application	Vserver	Linux-vserver	1.3.4	All	All	All
Application	Vserver	Linux-vserver	1.3.5	All	All	All
Application	Vserver	Linux-vserver	1.3.6	All	All	All
Application	Vserver	Linux-vserver	1.3.7	All	All	All
Application	Vserver	Linux-vserver	1.3.8	All	All	All
Application	Vserver	Linux-vserver	1.3.9	All	All	All
Application	Vserver	Linux-vserver	1.9.1	All	All	All

References

Reference	Source	Link
Linux VServer Project ProcFS Weak Sharing Permissions Vulnerability	BID	www.securityfocus.com/bid/20040703
20040703 Linux Virtual Server/Secure Context procs shared permissions flaw	BUGTRAQ	archives.neohapsis.com/archives/bugtraq/200407030001.html
Change Log - Linux-VServer	MISC	linux-vserver.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Secunia - Advisories - Linux VServer procs Permission Weakness	SECUNIA	secunia.com
7480	OSVDB	www.osvdb.org
SecurityTracker.com Archives - Linux VServer procs Permission Flaw Lets Local Users Change Permissions	SECTRACK	securitytracker.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)