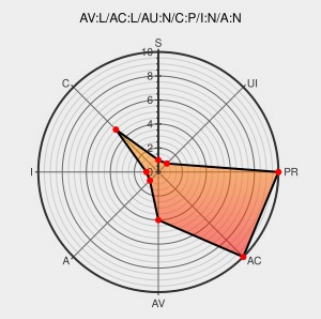
CVE-2006-2110

Published on: 05/01/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-2110

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Vserver from Virtual Private Server contain the following vulnerability:

Virtual Private Server (Vserver) 2.0.x before 2.0.2-rc18 and 2.1.x before 2.1.1-rc18 provides certain context capabilities (ccaps) that allow local guest users to perform operations that were only intended to be allowed by the guest-root.

CVE-2006-2110 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
/vserver-sources/2.0.1-r4/4915_vs2.0.1-vxcapable-fix.patch - Gentoo VPS project - Trac	Patch, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM dev.croup.de/proj/gentoo-vps/browser/vserver-sources/2.0.1-r4/4915_vs2.0.1-vxcapable-fix.patch
[Vserver] [SECURITY] ccaps not limited to root inside a guest	Exploit, Patch, list.linux-vserver.org, text/html	MLIST [Vserver] 20060428 [SECURITY] ccaps not limited to root inside a guest
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-1661
Linux-VServer Local Insecure Guest Context Capabilities Vulnerability	cve.report (archive), text/html	BID 17842
Debian -- Security Information -- DSA-1060-1	www.debian.org	DEBIAN DSA-1060

kernel-patch-vserver	Depreciated Link text/html	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF linux-vserver-ccaps-privilege-escalation(26285)
Debian update for kernel-patch-vserver - Advisories - Secunia	web.archive.org text/html	SECUNIA 20206
Linux-VServer "ccaps" Insecure Capabilities Security Issue - Advisories - Secunia	web.archive.org text/html	SECUNIA 19961

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Virtual Private Server	Vserver	2.0.2	All	All	All
Application	Virtual Private Server	Vserver	2.1.1	All	All	All
Application	Virtual Private Server	Vserver	2.0.2	All	All	All
Application	Virtual Private Server	Vserver	2.1.1	All	All	All

cpe:2.3:a:virtual_private_server:vserver:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:virtual_private_server:vserver:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:virtual_private_server:vserver:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:virtual_private_server:vserver:2.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→