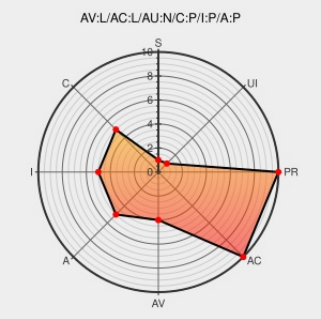
CVE-2004-2610

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2610

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



Certain versions of Mntd from Stefan Bambach contain the following vulnerability:

mntd_mount.c in mntd before 0.4.2 might allow local users to gain privileges via shell metacharacters in a remount option in the configuration file. NOTE: It is not clear whether this is a vulnerability because there is not necessarily any common usage in which privilege boundaries are crossed. Typical usage would restrict write access to the configuration file.

CVE-2004-2610 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
mntd Lack of Input Validation in Reading Configuration File May Let Local Users Execute Commands - SecurityTracker	Exploit, securitytracker.com, text/html	SECTRACK 1011088
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF mntd-read-configuration-gain-privileges(17149)
No Description Provided	Patch, www.osvdb.org, Inactive Link, Not Archived	OSVDB 9380
Download Mnt Daemon from SourceForge.net	Patch, prdownloads.sourceforge.net	CONFIRM prdownloads.sourceforge.net/mntd/mntd-

application/gzip

0.4.2.tar.gz?download

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	Stefan Bambach	Mntd	0.3.4	All	All	All
Application	Stefan Bambach	Mntd	0.3.5	All	All	All
Application	Stefan Bambach	Mntd	0.4.0	All	All	All
Application	Stefan Bambach	Mntd	0.4.1	All	All	All
Application	Stefan Bambach	Mntd	0.3.4	All	All	All
Application	Stefan Bambach	Mntd	0.3.5	All	All	All
Application	Stefan Bambach	Mntd	0.4.0	All	All	All
Application	Stefan Bambach	Mntd	0.4.1	All	All	All

cpe:2.3:a:stefan_bambach:mntd:0.3.4:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.3.5:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.4.0:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.4.1:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.3.4:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.3.5:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.4.0:*:*:*:*:*:*:*

cpe:2.3:a:stefan_bambach:mntd:0.4.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report