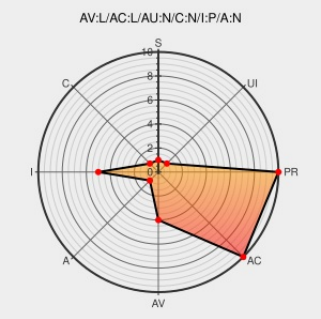
CVE-2003-1233

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1233

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



Certain versions of Integrity Protection Driver from Pedestal Software contain the following vulnerability:

Pedestal Software Integrity Protection Driver (IPD) 1.3 and earlier allows privileged attackers, such as rootkits, to bypass file access restrictions to the Windows kernel by using the NtCreateSymbolicLinkObject function to create a symbolic link to (1) \Device\PhysicalMemory or (2) to a drive letter using the subst command.

CVE-2003-1233 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**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	Exploit, Patch, archives.neohapsis.com, Inactive Link, Not Archived	BUGTRAQ 20030103 Another way to bypass Integrity Protection Driver ('subst' vuln)
No Description Provided	Patch, archives.neohapsis.com, Inactive Link, Not Archived	BUGTRAQ 20030103 Pedestal Software Security Notice
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF ipd-ntcreatesymboliclinkobject-subs-symlink(10979)

Secunia - Advisories - Integrity Protection Driver bypass	Patch Vendor Advisory web.archive.org text/html	SECUNIA 7816
Pedestal Software Integrity Protection Driver Symbolic Link Bypass Vulnerability	Patch cve.report (archive) text/html	BID 6511
www.phrack.org	web.archive.org text/html Inactive Link Not Archived	MISC www.phrack.org/show.php?p=59&a=16

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	Pedestal Software	Integrity Protection Driver	1.2	All	All	All
Application	Pedestal Software	Integrity Protection Driver	1.3	All	All	All
Application	Pedestal Software	Integrity Protection Driver	1.2	All	All	All
Application	Pedestal Software	Integrity Protection Driver	1.3	All	All	All

cpe:2.3:a:pedestal_software:integrity_protection_driver:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:pedestal_software:integrity_protection_driver:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:pedestal_software:integrity_protection_driver:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:pedestal_software:integrity_protection_driver:1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→