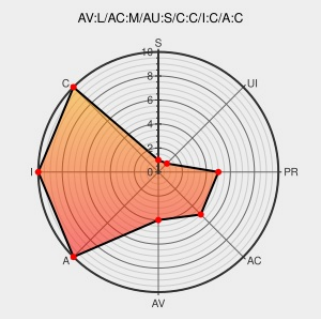
CVE-2006-6730

Published on: 12/26/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:04 PM UTC

CVE-2006-6730

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



Certain versions of Netbsd from Netbsd contain the following vulnerability:

OpenBSD and NetBSD permit usermode code to kill the display server and write to the X.Org /dev/xf86 device, which allows local users with root privileges to reduce securelevel by replacing the System Management Mode (SMM) handler via a write to an SMRAM address within /dev/xf86 (aka the video card memory-mapped I/O range), and then launching the new handler via a System Management Interrupt (SMI), as demonstrated by a write to Programmed I/O port 0xB2.

CVE-2006-6730 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	www.cansecwest.com application/vnd.ms-powerpoint	MISC www.cansecwest.com/slides06/csw06-duflot.ppt
Using CPU System Management Mode to Circumvent Operating System Security Functions | Agence nationale de la sécurité des systèmes d'information	www.ssi.gouv.fr application/pdf	MISC www.ssi.gouv.fr/fr/sciences/fichiers/lti/cansecwest2006-duflot-paper.pdf
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061215 Re: The (in)security of Xorg and DRI
[Xorg] DRI merging	lists.freedesktop.org	MLIST [Xorg] 20040613 DRI merging

	text/html	
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061214 The (in)security of Xorg and DRI
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20061218 Re: The (in)security of Xorg and DRI

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
Operating System	Netbsd	Netbsd	2.0.4	All	All	All
Operating System	Netbsd	Netbsd	2.0.4	All	All	All
Operating System	Openbsd	Openbsd	All	All	All	All
Operating System	Openbsd	Openbsd	All	All	All	All

cpe:2.3:o:netbsd:netbsd:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:netbsd:netbsd:2.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:*:*:*:*:*:*:*:*:

cpe:2.3:o:openbsd:openbsd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→