CVE-2011-4326

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-4326
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-17 11:00:00 UTC
Updated	2023-02-13 01:21:00 UTC
Description	The udp6_ufo_fragment function in net/ipv6/udp.c in the Linux kernel before 2.6.39, when a certain UDP Fragmentation Off

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Avaya	96x1 Ip Deskphone	-	All	All	All
Hardware	Avaya	96x1 Ip Deskphone	-	All	All	All
Operating System	Avaya	96x1 Ip Deskphone Firmware	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: CVE Request -- kernel: wrong headroom check in udp6_ufo_fragment()	MLIST	www.openwall.com	Mailing
Red Hat Customer Portal	MISC	access.redhat.com	
ipv6: udp: fix the wrong headroom check · torvalds/linux@a9cf73e · GitHub	CONFIRM	github.com	Patch,
ASA-2012-044 (WIND00319165 WIND00319166)	CONFIRM	downloads.avaya.com	Third P
Linux Kernel Headroom Check 'udp6_ufo_fragment()' Remote Denial of Service Vulnerability	BID	www.securityfocus.com	Third P
Bug 682066 – panic on ipv6 udp-fragmentation-offload of bridge device	CONFIRM	bugzilla.redhat.com	Exploit
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Patch,
404 Not Found	CONFIRM	ftp.osuosl.org	Broken

Bug 755584 – CVE-2011-4326 kernel: wrong headroom check in udp6_ufo_fragment()	CONFIRM	bugzilla.redhat.com	Issue T
Red Hat Customer Portal	MISC	access.redhat.com	
CVE-2011-4326 - Red Hat Customer Portal	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.