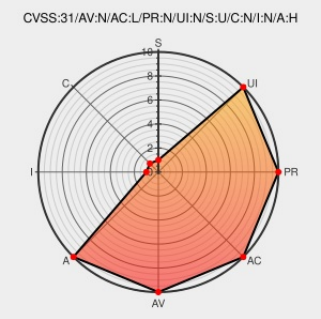
CVE-2011-2699

Published on: 05/24/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:31:00 AM UTC

CVE-2011-2699

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



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The IPv6 implementation in the Linux kernel before 3.1 does not generate Fragment Identification values separately for each destination, which makes it easier for remote attackers to cause a denial of service (disrupted networking) by predicting these values and sending crafted packets.

CVE-2011-2699 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Bug 723429 – CVE-2011-2699 kernel: ipv6: make fragment identifications	Issue Tracking Patch Third Party Advisory	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=723429

less predictable	bugzilla.redhat.com text/html	
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1
Solaris Multiple Bugs Let Remote Users Access and Modify Data and Deny Service and Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1027274
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=87c48fa3b4630905f98268dde838ee43626a060c
ipv6: make fragment identifications less predictable · torvalds/linux@87c48fa · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/87c48fa3b4630905f98268dde838ee43626a060c
Support / Security / Advisories / / MDVSA-2013:150 | Mandriva	Broken Link www.mandriva.com text/html	MANDRIVA MDVSA-2013:150
oss-security - Re: CVE request: kernel: ipv6: make fragment identifications less predictable	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110720 Re: CVE request: kernel: ipv6: make fragment identifications less predictable

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating	Redhat	Enterprise Mrg	2.0	All	All	All

System						
Application	Redhat	Enterprise Mrg	2.0	All	All	All

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→