CVE-2013-4588

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

Summary

CVE	CVE-2013-4588
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-11-20 13:19:00 UTC
Updated	2023-02-13 04:48:00 UTC
Description	Multiple stack-based buffer overflows in net/netfilter/ipvs/ip_vs_ctl.c in the Linux kernel before 2.6.33, when CONFIG_IP_VS

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	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
ipvs: Add boundary check on ioctl arguments · torvalds/linux@04bcef2 · GitHub	CONFIRM	github.com	Patch, Third Party A
ftp.linux.org.uk/pub/linux/linux-2.6/ChangeLog-2.6.33	CONFIRM	ftp.linux.org.uk	Broken Link
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
USN-2065-1: Linux kernel (EC2) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
USN-2064-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
oss-security - Re: CVE request: Linux kernel: net: ipvs stack buffer overflow	MLIST	www.openwall.com	Mailing List, Patch,
Bug 1030800 – CVE-2013-4588 Kernel: net: ipvs: stack buffer overflow	CONFIRM	bugzilla.redhat.com	Issue Tracking, Patc
Linux Kernel IP Virtual Server Multiple Stack Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	Third Party Advisory
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Patch, Vendor Advis
CVE Program record	CVE.ORG	www.cve.org	canonical

NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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