CVE-2020-8835

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8835
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-02 18:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-

Risk And Classification

Problem Types: CWE-125 | CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	8300	-	All	All	All
Operating System	Netapp	8300 Firmware	-	All	All	All
Hardware	Netapp	8700	-	All	All	All
Operating System	Netapp	8700 Firmware	-	All	All	All
Hardware	Netapp	A220	-	All	All	All
Operating System	Netapp	A220 Firmware	-	All	All	All
Hardware	Netapp	A320	-	All	All	All

Operating System	Netapp	A320 Firmware	-	All	All	All
Hardware	Netapp	A400	-	All	All	All
Operating System	Netapp	A400 Firmware	-	All	All	All
Hardware	Netapp	A700s	-	All	All	All
Operating System	Netapp	A700s Firmware	-	All	All	All
Hardware	Netapp	A800	-	All	All	All
Operating System	Netapp	A800 Firmware	-	All	All	All
Hardware	Netapp	C190	-	All	All	All
Operating System	Netapp	C190 Firmware	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	Fas2720	-	All	All	All
Operating System	Netapp	Fas2720 Firmware	-	All	All	All
Hardware	Netapp	Fas2750	-	All	All	All
Operating System	Netapp	Fas2750 Firmware	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H610c	-	All	All	All
Operating System	Netapp	H610c Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H615c	-	All	All	All
Operating System	Netapp	H615c Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All

Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 30 Update: kernel-tools-5.5.16-100.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[PATCH bpf-next 0/3] Fix __reg_bound_offset32 handling	CONFIRM	lore.kernel.org
[PATCH bpf-next 0/3] Fix __reg_bound_offset32 handling		lore.kernel.org
[SECURITY] Fedora 31 Update: kernel-5.5.15-200.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: kernel-5.6.2-300.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
oss-security - CVE-2021-33909: size_t-to-int vulnerability in Linux's filesystem layer	MLIST	www.openwall.com
[SECURITY] Fedora 32 Update: kernel-5.6.2-300.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: kernel-5.5.15-200.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
April 2020 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
kernel/git/netdev/net-next.git - Netdev Group's -next networking tree	CONFIRM	git.kernel.org
oss-security - CVE-2020-8835: Linux kernel bpf incorrect verifier vulnerability	CONFIRM	www.openwall.com
Zero Day Initiative — Pwn2Own 2020 – Day One Results	CONFIRM	www.thezdi.com
[SECURITY] Fedora 30 Update: kernel-tools-5.5.16-100.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-4313-1: Linux kernel vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-4313-1: Linux kernel vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Manfred Paul

LEGACY: Anatoly Trosinenko

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

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