CVE-2021-38166

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-38166
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-07 18:15:00 UTC
Updated	2023-11-07 03:37:00 UTC
Description	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many

Risk And Classification

Problem Types: CWE-787 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	T
CVE-2021-38166 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] Fedora 34 Update: kernel-5.13.10-200.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
kernel/git/bpf/bpf.git - BPF kernel tree	MISC	git.kernel.org	
FEDORA-2021-f35f45a76f	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: kernel-5.13.10-100.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[PATCH v2] bpf: Fix integer overflow involving bucket_size - Tatsuhiko Yasumatsu	MISC	lore.kernel.org	
Debian -- Security Information -- DSA-4978-1 linux	DEBIAN	www.debian.org	
[PATCH v2] bpf: Fix integer overflow involving bucket_size - Tatsuhiko Yasumatsu		lore.kernel.org	
[SECURITY] Fedora 33 Update: kernel-5.13.10-100.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178809 Debian Security Update for linux (DSA 4978-1)

184775 Debian Security Update for linux (CVE-2021-38166)

198524 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5096-1)

198540 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5113-1)

198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1)

281818 Fedora Security Update for kernel (FEDORA-2021-f35f45a76f)

281819 Fedora Security Update for kernel (FEDORA-2021-b22606e88b)

353155 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-005

610372 Google Pixel Android October 2021 Security Patch Missing

6140332 AWS Bottlerocket Security Update for kernel (GHSA-mjfv-5x2p-6cp6)

751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)

751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)

900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1

900302 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

900961 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6581-1)

903042 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5156)

906140 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5156-1)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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