



CVE-2021-29154

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-29154
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-08 21:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Cloud Backup	-	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	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

References

Reference

[SECURITY] Fedora 33 Update: kernel-5.11.13-200.fc33 - package-announce - Fedora Mailing-Lists

oss-security - [CVE-2021-29154] Linux kernel incorrect computation of branch displacements in BPF JIT compiler can be abused to execute a

[SECURITY] [DLA 2689-1] linux security update

[SECURITY] Fedora 33 Update: kernel-5.11.13-200.fc33 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2690-1] linux-4.19 security update

Kernel Live Patch Security Notice LSN-0076-1 ≈ Packet Storm

Linux kernel incorrect computation of branch displacements in BPF JIT compiler | Hacker News

Oracle Critical Patch Update Advisory - July 2022

CVE-2021-29154 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159179](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9222)

[159180](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9223)

[159277](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9306)

[159278](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9307)

[159375](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3327)

[159825](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)

[174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

[174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

[174925](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1248-1)

[174938](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1301-1)

178679 Debian Security Update for linux-4.19 (DLA 2690-1)
178680 Debian Security Update for linux (DLA 2689-1)
180424 Debian Security Update for linux (CVE-2021-29154)
198328 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4912-1)
198332 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4916-1)
198333 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4917-1)
239602 Red Hat Update for kernel-rt (RHSA-2021:3328)
239603 Red Hat Update for kernel (RHSA-2021:3327)
240275 Red Hat Update for kernel-rt (RHSA-2022:1975)
240298 Red Hat Update for kernel security (RHSA-2022:1988)
257109 CentOS Security Update for kernel (CESA-2021:3327)
281324 Fedora Security Update for kernel (FEDORA-2021-e71c033f88)
352274 Amazon Linux Security Advisory for kernel: ALAS2-2021-1627
352366 Amazon Linux Security Advisory for kernel: ALAS-2021-1503
353100 Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
353101 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
353102 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
353148 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-003
610351 Google Pixel Android July 2021 Security Patch Missing
6140141 AWS Bottlerocket Security Update for kernel (GHSA-6wm6-4q22-q7mf)
670416 EulerOS Security Update for kernel (EulerOS-SA-2021-1983)
670438 EulerOS Security Update for kernel (EulerOS-SA-2021-2062)
670449 EulerOS Security Update for kernel (EulerOS-SA-2021-2051)
670463 EulerOS Security Update for kernel (EulerOS-SA-2021-2221)
670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)
671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)
750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)

750014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)
750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
750031 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15) (SUSE-SU-2021:1728-1)
750032 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15 SP1) (SUSE-SU-2021:1715-1)
750034 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP1) (SUSE-SU-2021:1724-1)
750111 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 35 for SLE 12 SP3) (SUSE-SU-2021:1865-1)
750112 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 12 SP3) (SUSE-SU-2021:1870-1)
750199 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750261 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0579-1)
750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
900096 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901858 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6544-1)
903134 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4061)
906193 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4061-1)
940517 AlmaLinux Security Update for kernel (ALSA-2022:1988)

© [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 registered 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](#)