



CVE-2021-3444

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-3444
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-23 18:15:00 UTC
Updated	2021-12-02 19:37:00 UTC
Description	The bpf verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register w

Risk And Classification

Problem Types: CWE-125 | CWE-681

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
Kernel Live Patch Security Notice LSN-0082-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
Kernel Live Patch Security Notice LSN-0075-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
oss-security - [CVE-2021-3444] Linux kernel bpf verifier incorrect mod32 truncation	MISC	www.openwall.com	
oss-security - [CVE-2021-3444] Linux kernel bpf verifier incorrect mod32 truncation	MLIST	www.openwall.com	
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	lists.debian.org	
CVE-2021-3444 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica

Vendor Comments And Credit

Discovery Credit

LEGACY: De4dCr0w of 360 Alpha Lab

Legacy QID Mappings

159135 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9140)
159136 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9141)
174896 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)
174897 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)
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)
174950 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 21 for SLE 15) (SUSE-SU-2021:1344-1)
174952 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15) (SUSE-SU-2021:1347-1)
174953 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15 SP1) (SUSE-SU-2021:1395-1)
174955 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP1) (SUSE-SU-2021:1365-1)
178844 Debian Security Update for linux-4.19 (DLA 2785-1)
180357 Debian Security Update for linux (CVE-2021-3444)
198307 Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4887-1)
610351 Google Pixel Android July 2021 Security Patch Missing
670488 EulerOS Security Update for kernel (EulerOS-SA-2021-2246)
670514 EulerOS Security Update for kernel (EulerOS-SA-2021-2272)
670707 EulerOS Security Update for kernel (EulerOS-SA-2021-2465)
750001 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1572-1)
750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750005 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1595-1)
750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)

750199	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750276	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)
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)
900098	CBL-Mariner Linux Security Update for kernel 5.4.91
902793	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3986)

© [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](#)