



CVE-2021-3655

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

Summary

CVE	CVE-2021-3655
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 21:15:00 UTC
Updated	2022-10-27 12:29:00 UTC
Description	A vulnerability was found in the Linux kernel in versions prior to v5.14-rc1. Missing size validations on inbound SCTP packets.

Risk And Classification

Problem Types: CWE-20

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	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.14	-	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
1984024 – (CVE-2021-3655) CVE-2021-3655 kernel: missing size validations on inbound SCTP packets	MISC	bugzilla.redhat.com
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	lists.debian.org
[SECURITY] [DLA 2843-1] linux security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159402 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9458)

159403 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9459)
159404 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9460)
159424 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9485)
159427 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9488)
178844 Debian Security Update for linux-4.19 (DLA 2785-1)
178943 Debian Security Update for linux (DLA 2843-1)
179705 Debian Security Update for linux (CVE-2021-3655)
198562 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5136-1)
198569 Ubuntu Security Notification for Linux kernel (OEM 5.10) Vulnerabilities (USN-5139-1)
198586 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5162-1)
198587 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5163-1)
198588 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5161-1)
352503 Amazon Linux Security Advisory for kernel: ALAS2-2021-1696
352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
353143 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-008
353145 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-006
353156 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-004
353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036
353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037
353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038
390248 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0035)
610401 Google Android Devices March 2022 Security Patch Missing
610408 Google Android April 2022 Security Patch Missing for Huawei EMUI
610409 Google Android April 2022 Security Patch Missing for Samsung
6140304 AWS Bottlerocket Security Update for kernel (GHSA-p42f-xmmp-85vh)
671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688)
671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713)
671268 EulerOS Security Update for kernel (EulerOS-SA-2022-1196)

671344 EulerOS Security Update for kernel (EulerOS-SA-2022-1271)
671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)
751336 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1460-1)
751342 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3641-1)
751346 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3655-1)
751349 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1477-1)
751353 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3675-1)
751381 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3748-1)
751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)
751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)
751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)
900294 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
901115 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6576-1)
903126 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5154)
905803 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5154-1)

© [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 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](#)