



CVE-2020-25705

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

Summary

CVE	CVE-2020-25705
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-17 02:15:00 UTC
Updated	2021-05-18 12:15:00 UTC
Description	A flaw in ICMP packets in the Linux kernel may allow an attacker to quickly scan open UDP ports. This flaw allows an off-pa

Risk And Classification

Problem Types: CWE-330

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
Siemens Linux Based Products CISA	MISC	us-cert.cisa.g
CVE-2020-25705 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.neta
1894579 – (CVE-2020-25705) CVE-2020-25705 kernel: ICMP rate limiting can be used for DNS poisoning attack	MISC	bugzilla.redh
[SECURITY] [DLA 2494-1] linux security update	MLIST	lists.debian.c
cert-portal.siemens.com/productcert/pdf/ssa-324955.pdf	CONFIRM	cert-portal.si
[SECURITY] [DLA 2483-1] linux-4.19 security update	MLIST	lists.debian.c
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

[239151](#) Red Hat Update for kernel (RHSA-2021:0856)

[239344](#) Red Hat Update for kernel (RHSA-2021:1531)

[239456](#) Red Hat Update for kernel-rt (RHSA-2021:0774)

[257070](#) CentOS Security Update for kernel (CESA-2021:0856)

[296059](#) Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)

[352301](#) Amazon Linux Security Advisory for kernel: ALAC2012-2021-021

[352302](#) Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-022

[352303](#) Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-023

[376567](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux kernel Vulnerability (K09604370)

[376629](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) TMM Vulnerability (K41440465)

[377038](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)

[390217](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)

[390234](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0001)

[43856](#) Hewlett Packard Enterprise (HPE) ArubaOS SAD Domain Name System (DNS) Side Channel Vulnerability (ARUBA-PSA-2021-008)

[591192](#) Siemens Linux-based Products (Update J) Vulnerability (ICSA-21-131-03, SSA-324955)

[610331](#) Google Android Devices April 2021 Security Patch Missing

[610340](#) Google Android May 2021 Security Patch Missing for Samsung

[610341](#) Google Android May 2021 Security Patch Missing for LGE

[610347](#) Google Android May 2021 Security Patch Missing for Huawei EMUI

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[750488](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)

[750518](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2161-1)

[750533](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)

[750568](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2034-1)

750738 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3326-1)
900040 CBL-Mariner Linux Security Update for kernel 5.4.91
902876 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3627)
905748 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3627-1)
940408 AlmaLinux Security Update for kernel (ALSA-2021:0558)

© [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](#)