



CVE-2020-13529

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

Summary

CVE	CVE-2020-13529
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-10 16:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can c

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Freedesktop	Systemd	245	-	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Systemd Project	Systemd	245	-	All	All

References

Reference	Source	Link	Ta
TALOS-2020-1142 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
oss-security - Re: Pop!_OS Membership to linux-distros list	MLIST	www.openwall.com	
oss-security - Re: Pop!_OS Membership to linux-distros list	MLIST	www.openwall.com	
FEDORA-2021-166e461c8d	FEDORA	lists.fedoraproject.org	
oss-security - Re: Pop!_OS Membership to linux-distros list	MLIST	www.openwall.com	
systemd: Multiple vulnerabilities (GLSA 202107-48) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 33 Update: systemd-246.15-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE-2020-13529 Systemd Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	

CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159494 Oracle Enterprise Linux Security Update for NetworkManager (ELSA-2021-4361)
198434 Ubuntu Security Notification for systemd vulnerabilities (USN-5013-1)
239783 Red Hat Update for networkmanager security (RHSA-2021:4361)
281739 Fedora Security Update for systemd (FEDORA-2021-166e461c8d)
354074 Amazon Linux Security Advisory for systemd : ALAS2-2022-1854
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
670821 EulerOS Security Update for systemd (EulerOS-SA-2021-2700)
670837 EulerOS Security Update for systemd (EulerOS-SA-2021-2725)
670979 EulerOS Security Update for systemd (EulerOS-SA-2021-2647)
671009 EulerOS Security Update for NetworkManager (EulerOS-SA-2021-2665)
671030 EulerOS Security Update for systemd (EulerOS-SA-2021-2676)
671242 EulerOS Security Update for NetworkManager (EulerOS-SA-2022-1178)
671243 EulerOS Security Update for systemd (EulerOS-SA-2022-1192)
710021 Gentoo Linux systemd Multiple vulnerabilities (GLSA 202107-48)
751002 OpenSUSE Security Update for systemd (openSUSE-SU-2021:2809-1)
940228 AlmaLinux Security Update for NetworkManager (ALSA-2021:4361)
960880 Rocky Linux Security Update for NetworkManager (RLSA-2021:4361)

© 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