CVE-2022-2526

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-2526
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-09 15:15:00 UTC
Updated	2023-01-20 03:17:00 UTC
Description	A use-after-free vulnerability was found in systemd. This issue occurs due to the on_stream_io() function and dns_stream_

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Active Iq Unified Manager	-	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	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Systemd Project	Systemd	240	All	All	All

References

Reference	Source	Link	Tags
resolved: pin stream while calling callbacks for it · systemd/systemd@d973d94 · GitHub	MISC	github.com	
CVE-2022-2526 Systemd Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 160061 Oracle Enterprise Linux Security Update for systemd (ELSA-2022-6160)
- 160071 Oracle Enterprise Linux Security Update for systemd (ELSA-2022-6206)
- 180952 Debian Security Update for systemd (CVE-2022-2526)
- 198914 Ubuntu Security Notification for systemd Vulnerability (USN-5583-1)
- 240625 Red Hat Update for systemd (RHSA-2022:6162)
- 240630 Red Hat Update for systemd (RHSA-2022:6160)
- 240633 Red Hat Update for systemd (RHSA-2022:6161)
- 240640 Red Hat Update for systemd (RHSA-2022:6206)
- 257191 CentOS Security Update for systemd (CESA-2022:6160)
- 354074 Amazon Linux Security Advisory for systemd : ALAS2-2022-1854
- 672151 EulerOS Security Update for systemd (EulerOS-SA-2022-2450)
- 672586 EulerOS Security Update for systemd (EulerOS-SA-2023-1339)
- 904843 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd-bootstrap (12450)
- 904847 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (12447)
- 940650 AlmaLinux Security Update for systemd (ALSA-2022:6206)
- 960169 Rocky Linux Security Update for systemd (RLSA-2022:6206)

© 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 registred 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