



CVE-2022-3821

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

Summary

CVE	CVE-2022-3821
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-08 22:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply s

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Systemd Project	Systemd	All	All	All	All

References

Reference	Source	Link
time-util: fix buffer-over-run · systemd/systemd@9102c62 · GitHub	MISC	github.com
time-util: fix buffer-over-run by yuwata · Pull Request #23933 · systemd/systemd · GitHub	MISC	github.com
systemd: Multiple Vulnerabilities (GLSA 202305-15) — Gentoo security	GENTOO	security.gentoo.org
2139327 – (CVE-2022-3821) CVE-2022-3821 systemd: buffer overrun in format_timespan() function.	MISC	bugzilla.redhat.com
[SECURITY] [DLA 3474-1] systemd security update	MLIST	lists.debian.org
Buffer overrun in format_timespan · Issue #23928 · systemd/systemd · GitHub	MISC	github.com
[SECURITY] Fedora 35 Update: systemd-249.13-6.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 35 Update: systemd-249.13-6.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.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

160393 Oracle Enterprise Linux Security Update for systemd (ELSA-2023-0100)
160436 Oracle Enterprise Linux Security Update for systemd (ELSA-2023-0336)
183976 Debian Security Update for systemd (CVE-2022-3821)
199221 Ubuntu Security Notification for systemd Vulnerabilities (USN-5928-1)
241060 Red Hat Update for systemd (RHSA-2023:0100)
241105 Red Hat Update for systemd (RHSA-2023:0336)
243029 Red Hat Update for systemd (RHSA-2024:1105)
283326 Fedora Security Update for systemd (FEDORA-2022-8ac4104a02)
354127 Amazon Linux Security Advisory for systemd : ALAS2-2022-1899
378048 Alibaba Cloud Linux Security Update for systemd (ALINUX3-SA-2023:0025)
6000052 Debian Security Update for systemd (DLA 3474-1)
672486 EulerOS Security Update for systemd (EulerOS-SA-2023-1048)
672513 EulerOS Security Update for systemd (EulerOS-SA-2023-1023)
672536 EulerOS Security Update for systemd (EulerOS-SA-2023-1115)
672542 EulerOS Security Update for systemd (EulerOS-SA-2023-1139)
672586 EulerOS Security Update for systemd (EulerOS-SA-2023-1339)
672600 EulerOS Security Update for networkmanager (EulerOS-SA-2023-1329)
672620 EulerOS Security Update for systemd (EulerOS-SA-2023-1402)
672661 EulerOS Security Update for systemd (EulerOS-SA-2023-1374)
710708 Gentoo Linux systemd Multiple Vulnerabilities (GLSA 202305-15)
752804 SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2022:3999-1)
752897 SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2022:4056-1)
752955 SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2022:4279-1)
753894 SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2023:1776-1)
904487 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (11447)

904500 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (11443)
904626 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (11447-1)
904643 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (11443-1)
940878 AlmaLinux Security Update for systemd (ALSA-2023:0100)
940903 AlmaLinux Security Update for systemd (ALSA-2023:0336)
960634 Rocky Linux Security Update for systemd (RLSA-2023:0336)

© [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](#)