



# CVE-2021-3997

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

## Summary

<b>CVE</b>	CVE-2021-3997
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-23 20:15:00 UTC
<b>Updated</b>	2023-05-03 12:15:00 UTC
<b>Description</b>	A flaw was found in systemd. An uncontrolled recursion in systemd-tmpfiles may lead to a denial of service at boot time wh

## Risk And Classification

**Problem Types:** CWE-674

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Systemd Project</a>	<a href="#">Systemd</a>	All	All	All	All

## References

Reference	Source	Link
systemd: Multiple Vulnerabilities (GLSA 202305-15) — Gentoo security	GENTOO	<a href="#">securi</a>
shared/rm-rf: loop over nested directories instead of instead of recu... · systemd/systemd@5b1cf7a · GitHub	MISC	<a href="#">github</a>
2024639 – (CVE-2021-3997) CVE-2021-3997 systemd: Uncontrolled recursion in systemd-tmpfiles when removing files	MISC	<a href="#">bugzill</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
oss-security - CVE-2021-3997: Uncontrolled recursion in systemd's systemd-tmpfiles	MISC	<a href="#">www.c</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

179586	Debian Security Update for systemd (CVE-2021-3997)
198629	Ubuntu Security Notification for systemd Vulnerability (USN-5226-1)
282242	Fedora Security Update for systemd (FEDORA-2022-f38f479b8f)
282293	Fedora Security Update for systemd (FEDORA-2022-af1728fea9)
354291	Amazon Linux Security Advisory for systemd : ALAS2022-2022-219
354395	Amazon Linux Security Advisory for systemd : ALAS2022-2022-052
354518	Amazon Linux Security Advisory for systemd : ALAS2022-2022-040
354567	Amazon Linux Security Advisory for systemd : ALAS-2022-219
355284	Amazon Linux Security Advisory for systemd : ALAS2023-2023-025
376419	Snap-Confine Local Privilege Escalation Vulnerability (Oh Snap! More Lemmings)
591406	Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
671469	EulerOS Security Update for systemd (EulerOS-SA-2022-1439)
671483	EulerOS Security Update for systemd (EulerOS-SA-2022-1460)
671486	EulerOS Security Update for systemd (EulerOS-SA-2022-1497)
671489	EulerOS Security Update for systemd (EulerOS-SA-2022-1516)
710708	Gentoo Linux systemd Multiple Vulnerabilities (GLSA 202305-15)
751593	OpenSUSE Security Update for systemd (openSUSE-SU-2022:0043-1)
751736	OpenSUSE Security Update for systemd (openSUSE-SU-2022:0539-1)
751998	SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2022:0043-1)
752002	SUSE Enterprise Linux Security Update for systemd (SUSE-SU-2022:0539-1)
903771	Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (10648)

© [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](#).

