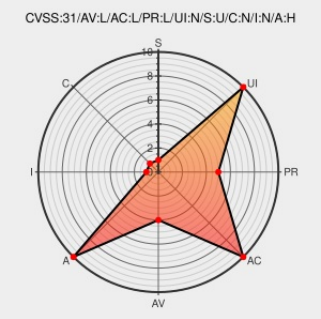
CVE-2022-45873

Published on: Not Yet Published

Last Modified on: 12/01/2022 02:33:00 PM UTC

CVE-2022-45873

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Systemd from Systemd Project contain the following vulnerability:

systemd 250 and 251 allows local users to achieve a systemd-coredump deadlock by triggering a crash that has a long backtrace. This occurs in parse_elf_object in shared/elf-util.c. The exploitation methodology is to crash a binary calling the same function recursively, and put it in a deeply nested directory to make its backtrace large enough to cause the deadlock. This must be done 16 times when MaxConnections=16 is set for the systemd/units/systemd-coredump.socket file.

CVE-2022-45873 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Fix coredump deadlock with overly long backtraces by keszybz · Pull Request #25055 · systemd/systemd · GitHub	github.com text/html	MISC github.com/systemd/systemd/pull/25055#issuecomment-1313733553
resolved: various monitor fixes by poettering · Pull Request #24853 · systemd/systemd · GitHub	github.com text/html	MISC github.com/systemd/systemd/pull/24853#issuecomment-1326561497
coredump: avoid deadlock when passing processed backtrace data · systemd/systemd@076b807 ·	github.com text/html	MISC github.com/systemd/systemd/commit/076b807be472630692c5348c60d0c2b7b28ad437

GitHub

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

904614 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (11523)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Systemd Project	Systemd	252	rc1	All	All
Application	Systemd Project	Systemd	252	rc2	All	All
Application	Systemd Project	Systemd	All	All	All	All

cpe:2.3:a:systemd_project:systemd:252:rc1:*:*:*:*:*:*:

cpe:2.3:a:systemd_project:systemd:252:rc2:*:*:*:*:*:*:

cpe:2.3:a:systemd_project:systemd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-45873 : systemd 250 and 251 allows local users to achieve a systemd-coredump deadlock by triggering a cras… twitter.com/i/web/status/1…	2022-11-23 23:02:43
/r/netcve	CVE-2022-45873	2022-11-23 23:38:46

← Previous ID

Next ID→