Systemd-coredump: race condition that allows a local attacker to crash a suid program and gain read access to the resulting core dump

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-4598
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-30 14:15:23 UTC
Updated	2026-05-12 13:17:21 UTC
Description	A vulnerability was found in systemd-coredump. This flaw allows an attacker to force a SUID process to crash and replace i

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-364 | CWE-364 Signal Handler Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Systemd Project	Systemd	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:252-55.el9_7.7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:252-55.el9_7.7 * rpm
CNA	Red Hat	Red Hat Ceph Storage 7	unaffected sha256:cfaf2a3c9513bd280265b0e2ca5f7d60022a2e36202
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:b09eb0a1d99e655de562919ded095bbb5dc65961e3
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:97a60239048123bc963d7c9ac2ad85caa6a254759e
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:d4e8987a100ea60942306f1564679e51fa1364f6124
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:899bd7f941512d54af8ab369ca03028a7d27d05887c
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:1d72e553fe5a7696e600dc8fd2fe9050ba1992fa190b
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom

References

Reference	Source	Link
access.redhat.com/errata/RHSA-2025:22660	secalert@redhat.com	access.redhat.com
www.openwall.com/lists/oss-security/2025/06/05/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
www.openwall.com/lists/oss-security/2025/08/18/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
www.openwall.com/lists/oss-security/2025/06/05/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
seclists.org/fulldisclosure/2025/Jun/9	af854a3a-2127-422b-91ae-364da2661108	seclists.org
ciq.com/blog/the-real-danger-of-systemd-coredump-cve-2025-4598	af854a3a-2127-422b-91ae-364da2661108	ciq.com
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
access.redhat.com/errata/RHSA-2026:1652	secalert@redhat.com	access.redhat.com
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com
access.redhat.com/errata/RHSA-2025:23234	secalert@redhat.com	access.redhat.com
www.openwall.com/lists/oss-security/2025/08/18/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
access.redhat.com/errata/RHSA-2025:22868	secalert@redhat.com	access.redhat.com
lists.debian.org/debian-lts-announce/2025/07/msg00022.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
blogs.oracle.com/linux/post/analysis-of-cve-2025-4598	af854a3a-2127-422b-91ae-364da2661108	blogs.oracle.com
access.redhat.com/security/cve/CVE-2025-4598	secalert@redhat.com	access.redhat.com
www.openwall.com/lists/oss-security/2025/05/29/3	secalert@redhat.com	www.openwall.com
access.redhat.com/errata/RHSA-2025:23227	secalert@redhat.com	access.redhat.com
access.redhat.com/errata/RHSA-2026:0414	secalert@redhat.com	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-05-29T19:04:54.578Z	Reported to Red Hat.
CNA	2025-05-29T00:00:00.000Z	Made public.

Workarounds

CNA: This issue can be mitigated by disabling the capability of the system to generate a coredump for SUID binaries. The perform that, the following command can be ran as `root` user: ~~~ echo 0 > /proc/sys/fs/suid_dumpable ~~~ While this mitigates this vulnerability while it's not possible to update the systemd package, it disables the capability of analyzing crashes for such binaries.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**