CVE-2020-1712

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-1712
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-31 17:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are p

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Freedesktop	Systemd	All	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All
Application	Redhat	Discovery	-	All	All	All
Application	Redhat	Discovery	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Migration Toolkit	1.0	All	All	All
Application	Redhat	Migration Toolkit	1.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Systemd Project	Systemd	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3063-1] systemd security update	MLIST	lists.de

polkit: when authorizing via PK let's re-resolve callback/userdata in… · systemd/systemd@6374862 · GitHub	CONFIRM	github.
Merge branch 'polkit-ref-count' · systemd/systemd@ea0d0ed · GitHub	CONFIRM	github.
1794578 – (CVE-2020-1712) CVE-2020-1712 systemd: use-after-free when asynchronous polkit queries are performed	CONFIRM	bugzill
Fix typo in function name · systemd/systemd@bc130b6 · GitHub	CONFIRM	github.
sd-bus: introduce API for re-enqueuing incoming messages · systemd/systemd@1068447 · GitHub	CONFIRM	github.
oss-security - CVE-2020-1712 systemd: use-after-free when asynchronous polkit queries are performed	CONFIRM	www.o
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 180179 Debian Security Update for systemd (DLA 3063-1)
- 377123 Alibaba Cloud Linux Security Update for systemd (ALINUX3-SA-2022:0039)
- 591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- 900080 CBL-Mariner Linux Security Update for systemd 239
- 903171 Common Base Linux Mariner (CBL-Mariner) Security Update for systemd (1789)