



# CVE-2020-1712

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

## Summary

<b>CVE</b>	CVE-2020-1712
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-03-31 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:19:00 UTC
<b>Description</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Freedesktop</a>	<a href="#">Systemd</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ceph Storage</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ceph Storage</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Discovery</a>	-	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Discovery</a>	-	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>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Migration Toolkit</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Migration Toolkit</a>	1.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openshift Container Platform</a>	4.0	All	All	All
Application	<a href="#">Systemd Project</a>	<a href="#">Systemd</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 3063-1] systemd security update	MLIST	<a href="#">lists.de</a>

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

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

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

© [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](#)