



# CVE-2023-1981

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

## Summary

<b>CVE</b>	CVE-2023-1981
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-26 18:15:00 UTC
<b>Updated</b>	2023-06-02 19:06:00 UTC
<b>Description</b>	A vulnerability was found in the avahi library. This flaw allows an unprivileged user to make a dbus call, causing the avahi d

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Avahi</a>	<a href="#">Avahi</a>	0.7-20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	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

## References

Reference	Source	Link	Tags
<a href="#">avahi-daemon can be crashed via Dbus · Issue #375 · lathiat/avahi · GitHub</a>	MISC	<a href="#">github.com</a>	
<a href="#">2185911 – (CVE-2023-1981) CVE-2023-1981 avahi: avahi-daemon can be crashed via DBus</a>	MISC	<a href="#">bugzilla.redhat.com</a>	
<a href="#">cve-details</a>	MISC	<a href="#">access.redhat.com</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonical
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

161082 Oracle Enterprise Linux Security Update for avahi (ELSA-2023-6707)
161179 Oracle Enterprise Linux Security Update for avahi (ELSA-2023-7190)
181764 Debian Security Update for avahi (DLA 3414-1)
182541 Debian Security Update for avahi (CVE-2023-1981)
199388 Ubuntu Security Notification for Avahi Vulnerability (USN-6129-1)
199603 Ubuntu Security Notification for Avahi Vulnerability (USN-6129-2)
242395 Red Hat Update for avahi (RHSA-2023:6707)
242453 Red Hat Update for avahi (RHSA-2023:7190)
284183 Fedora Security Update for avahi (FEDORA-2023-16a1a6ec81)
355700 Amazon Linux Security Advisory for avahi : ALAS2-2023-2161
379643 Alibaba Cloud Linux Security Update for avahi (ALINUX3-SA-2024:0035)
510759 Alpine Linux Security Update for avahi
673184 EulerOS Security Update for avahi (EulerOS-SA-2023-2306)
673188 EulerOS Security Update for avahi (EulerOS-SA-2023-2326)
673223 EulerOS Security Update for avahi (EulerOS-SA-2023-2346)
673256 EulerOS Security Update for avahi (EulerOS-SA-2023-2372)
673717 EulerOS Security Update for avahi (EulerOS-SA-2023-2632)
673880 EulerOS Security Update for avahi (EulerOS-SA-2023-2674)
753936 SUSE Enterprise Linux Security Update for avahi (SUSE-SU-2023:1956-1)
753940 SUSE Enterprise Linux Security Update for avahi (SUSE-SU-2023:1993-1)
941371 AlmaLinux Security Update for avahi (ALSA-2023:6707)
941430 AlmaLinux Security Update for avahi (ALSA-2023:7190)
961078 Rocky Linux Security Update for avahi (RLSA-2023:7190)

© [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](https://status.cve.report)**