



CVE-2021-26720

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

Summary

CVE	CVE-2021-26720
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-17 22:15:00 UTC
Updated	2022-12-06 21:52:00 UTC
Description	avahi-daemon-check-dns.sh in the Debian avahi package through 0.8-4 is executed as root via /etc/network/if-up.d/avahi-d

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avahi	Avahi	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference

Bug 1180827 – VUL-0: CVE-2021-26720: avahi: outdated and insecure if-up script avahi-daemon-check-dns.sh
Bug #1870824 "Errors in script /usr/lib/avahi/avahi-daemon-check...": Bugs : avahi package : Ubuntu
Debian -- Details of package avahi-daemon in sid
404 Not Found
#982796 - buster-pu: package avahi/0.7-4 - Debian Bug report logs
[SECURITY] [DLA 3047-1] avahi security update
CVE-2021-26720
Debian -- Details of package avahi-daemon in buster
oss-security - CVE-2021-26720: avahi-daemon: 'avahi' to 'root' user privilege escalation through Debian specific if-up script avahi-daemon-che

Debian -- Details of package avahi-daemon in bullseye

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179359](#) Debian Security Update for avahi (DLA 3047-1)

[179993](#) Debian Security Update for avahi (CVE-2021-26720)

[750101](#) SUSE Enterprise Linux Security Update for avahi (SUSE-SU-2021:1845-1)

[750337](#) OpenSUSE Security Update for avahi (openSUSE-SU-2021:0370-1)

[750789](#) OpenSUSE Security Update for avahi (openSUSE-SU-2021:1845-1)

[901804](#) Common Base Linux Mariner (CBL-Mariner) Security Update for avahi (6323-1)

[906451](#) Common Base Linux Mariner (CBL-Mariner) Security Update for avahi (6323-2)

© [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](#)