



# CVE-2021-27803

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

## Summary

<b>CVE</b>	CVE-2021-27803
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-02-26 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:32:00 UTC
<b>Description</b>	A vulnerability was discovered in how p2p/p2p_pd.c in wpa_supplicant before 2.10 processes P2P (Wi-Fi Direct) provision c

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	All	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Wpa Supplicant</a>	All	All	All	All

## References

Reference	Source	Link
oss-security - wpa_supplicant P2P provision discovery processing vulnerability	MISC	<a href="http://www.openwall.com">www.openwall.com</a>
oss-security - Re: wpa_supplicant P2P provision discovery processing vulnerability	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
[SECURITY] Fedora 34 Update: wpa_supplicant-2.9-12.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
w1.fi/security/2021-1/0001-P2P-Fix-a-corner-case-in-peer-addition-b...	MISC	<a href="http://w1.fi">w1.fi</a>
[SECURITY] Fedora 33 Update: wpa_supplicant-2.9-8.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>

[SECURITY] [DLA 2581-1] wpa security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 33 Update: wpa_supPLICANT-2.9-8.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
w1.fi/security/2021-1/wpa_supPLICANT-p2p-provision-discovery-proces...	MISC	<a href="https://w1.fi">w1.fi</a>
[SECURITY] Fedora 32 Update: wpa_supPLICANT-2.9-6.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 32 Update: wpa_supPLICANT-2.9-6.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: wpa_supPLICANT-2.9-12.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-4898-1 wpa	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[174736](#) SUSE Enterprise Linux Security update for wpa\_supPLICANT (SUSE-SU-2021:0721-1)

[178562](#) Debian Security Update for wpa (DSA 4898-1)

[180140](#) Debian Security Update for wpa (CVE-2021-27803)

[239159](#) Red Hat Update for wpa\_supPLICANT (RHSA-2021:0808)

[257069](#) CentOS Security Update for wpa\_supPLICANT (CESA-2021:0808)

[281575](#) Fedora Security Update for wpa\_supPLICANT (FEDORA-2021-3430f96019)

[281576](#) Fedora Security Update for wpa\_supPLICANT (FEDORA-2021-9b00febe54)

[281577](#) Fedora Security Update for wpa\_supPLICANT (FEDORA-2021-99cad2b81f)

[352260](#) Amazon Linux Security Advisory for wpa\_supPLICANT: ALAS2-2021-1624

[377146](#) Alibaba Cloud Linux Security Update for wpa\_supPLICANT (ALINUX3-SA-2021:0019)

[377207](#) Alibaba Cloud Linux Security Update for wpa\_supPLICANT (ALINUX2-SA-2021:0013)

[43901](#) HP Printers Multiple Vulnerabilities (HPSBPI03782)

[500745](#) Alpine Linux Security Update for wpa\_supPLICANT

[501506](#) Alpine Linux Security Update for wpa\_supPLICANT

[501791](#) Alpine Linux Security Update for wpa\_supPLICANT

[504520](#) Alpine Linux Security Update for wpa\_supPLICANT

[670215](#) EulerOS Security Update for wpa\_supPLICANT (EulerOS-SA-2021-1860)

[670307](#) EulerOS Security Update for wpa\_supPLICANT (EulerOS-SA-2021-1917)

670332 EulerOS Security Update for wpa_supplicant (EulerOS-SA-2021-1892)
670681 EulerOS Security Update for wpa_supplicant (EulerOS-SA-2021-2439)
750323 OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2021:0404-1)
900158 CBL-Mariner Linux Security Update for wpa_supplicant 2.9
900870 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa_supplicant (6973-1)
903206 Common Base Linux Mariner (CBL-Mariner) Security Update for wpa_supplicant (3919)
940363 AlmaLinux Security Update for wpa_supplicant (ALSA-2021:0809)

© [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](#)**