



# CVE-2019-10064

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

## Summary

<b>CVE</b>	CVE-2019-10064
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-28 15:15:00 UTC
<b>Updated</b>	2022-01-01 19:31:00 UTC
<b>Description</b>	hostapd before 2.6, in EAP mode, makes calls to the rand() and random() standard library functions without any preceding

## Risk And Classification

**Problem Types:** CWE-331

## 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>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	All	All	All	All
Application	<a href="#">W1.fi</a>	<a href="#">Hostapd</a>	All	All	All	All

## References

Reference	Source	L
<a href="#">oss-security - Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)</a>	MLIST	w
<a href="#">Full Disclosure: Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)</a>	FULLDISC	si
<a href="#">oss-security - Re: Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)</a>	MLIST	w
<a href="#">Hostapd Insufficient Entropy ≈ Packet Storm</a>	MISC	p
<a href="#">[SECURITY] [DLA 2138-1] wpa security update</a>	MLIST	li
<a href="#">hostap - hostapd/wpa_suplicant</a>	MISC	w
<a href="#">[SECURITY] [DLA 2318-1] wpa security update</a>	MLIST	li
<a href="#">CVE Program record</a>	CVE.ORG	w
<a href="#">NVD vulnerability detail</a>	NVD	n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)