



CVE-2016-10743

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

Summary

CVE	CVE-2016-10743
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-23 19:29:00 UTC
Updated	2019-04-10 19:29:00 UTC
Description	hostapd before 2.6 does not prevent use of the low-quality PRNG that is reached by an os_random() function call.

Risk And Classification

Problem Types: CWE-332

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	W1.fi	Hostapd	All	All	All	All
Application	W1.fi	Hostapd	All	All	All	All

References

Reference	Source	L
oss-security - Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)	MLIST	w
Full Disclosure: Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)	FULLDISC	s
oss-security - Re: Hostapd fails at seeding PRNGS, leading to insufficient entropy (CVE-2016-10743 and CVE-2019-10064)	MLIST	w
Hostapd Insufficient Entropy ≈ Packet Storm	MISC	p
USN-3944-1: wpa_supplicant and hostapd vulnerabilities Ubuntu security notices	UBUNTU	u
[SECURITY] [DLA 1733-1] wpa security update	MLIST	li
hostap - hostapd/wpa_supplicant	MISC	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	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](#)