



CVE-2015-4143

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2015-4143 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2015-06-15 15:59:00 UTC |
| Updated | 2018-10-30 16:27:00 UTC |
| Description | The EAP-pwd server and peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 allows remote attackers to c |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------|---------|--------|---------|----------|
| Operating System | Openseuse | Openseuse | 13.1 | All | All | All |
| Operating System | Openseuse | Openseuse | 13.2 | All | All | All |
| Operating System | Openseuse | Openseuse | 13.1 | All | All | All |
| Operating System | Openseuse | Openseuse | 13.2 | All | All | All |
| Application | W1.fi | Hostapd | 1.0 | All | All | All |
| Application | W1.fi | Hostapd | 1.1 | All | All | All |
| Application | W1.fi | Hostapd | 2.0 | All | All | All |
| Application | W1.fi | Hostapd | 2.1 | All | All | All |
| Application | W1.fi | Hostapd | 2.2 | All | All | All |
| Application | W1.fi | Hostapd | 2.3 | All | All | All |
| Application | W1.fi | Hostapd | 2.4 | All | All | All |
| Application | W1.fi | Hostapd | 1.0 | All | All | All |
| Application | W1.fi | Hostapd | 1.1 | All | All | All |
| Application | W1.fi | Hostapd | 2.0 | All | All | All |
| Application | W1.fi | Hostapd | 2.1 | All | All | All |
| Application | W1.fi | Hostapd | 2.2 | All | All | All |
| Application | W1.fi | Hostapd | 2.3 | All | All | All |

| | | | | | | |
|-------------|-----------------------|--------------------------------|-----|-----|-----|-----|
| Application | W1.fi | Hostapd | 2.4 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 1.0 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 1.1 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.0 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.1 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.2 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.3 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.4 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 1.0 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 1.1 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.0 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.1 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.2 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.3 | All | All | All |
| Application | W1.fi | Wpa Supplicant | 2.4 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|-------------------------------------|---------------|
| w1.fi/security/2015-4/eap-pwd-missing-payload-length-validation.txt | CONFIRM | w1.fi | Vendor Advise |
| hostapd and wpa_supplicant: Multiple vulnerabilities (GLSA 201606-17) — Gentoo Security | GENTOO | security.gentoo.org | Third Party A |
| USN-2650-1: wpa_supplicant and hostapd vulnerabilities Ubuntu | UBUNTU | www.ubuntu.com | |
| oss-security - Re: CVE request: vulnerability in wpa_supplicant and hostapd | MLIST | www.openwall.com | |
| openSUSE-SU-2015:1030-1: moderate: Recommended update for wpa_supplicant | SUSE | lists.opensuse.org | Third Party A |
| oss-security - Re: CVE request: vulnerability in wpa_supplicant and hostapd | MLIST | www.openwall.com | |
| Debian -- Security Information -- DSA-3397-1 wpa | DEBIAN | www.debian.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ar |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[750549](#) OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2059-1)

[750557](#) OpenSUSE Security Update for wpa_supplicant (openSUSE-SU-2020:2053-1)

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](#)