



CVE-2019-11234

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2019-11234 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-04-22 11:29:00 UTC |
| Updated | 2019-05-13 18:29:00 UTC |
| Description | FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a "Dragonblood" issue, a sim |

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | All | All | All |
| Operating System | Fedoraproject | Fedora | All | All | All | All |
| Operating System | Fedoraproject | Fedora | All | All | All | All |
| Application | Freeradius | Freeradius | All | All | All | All |
| Application | Freeradius | Freeradius | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |

References

| Reference | Source | Link |
|---|--------|--|
| VU#871675 - WPA3 design issues and implementation vulnerabilities in hostapd and wpa_supplicant | MISC | www.kb.cert.org |
| Red Hat Customer Portal | REDHAT | access.redhat.com |

| | | |
|---|---------|---|
| [security-announce] openSUSE-SU-2019:1394-1: important: Security update | SUSE | lists.opensuse.org |
| [security-announce] openSUSE-SU-2019:1346-1: important: Security update | SUSE | lists.opensuse.org |
| USN-3954-1: FreeRADIUS vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | usn.ubuntu.com |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| papers.mathyvanhoef.com/dragonblood.pdf | MISC | papers.mathyvanhoe |
| Releases | MISC | freeradius.org |
| [security-announce] openSUSE-SU-2020:0542-1: important: Security update | SUSE | lists.opensuse.org |
| 1695783 – (CVE-2019-11234) CVE-2019-11234 freeradius: eap-pwd: fake authentication using reflection | CONFIRM | bugzilla.redhat.com |
| Releases | MISC | freeradius.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377182](#) Alibaba Cloud Linux Security Update for freeradius (ALINUX2-SA-2019:0031)

[378222](#) Virtuozzo Linux Security Update for freeradius-devel (VZLSA-2019:1131)

[500186](#) Alpine Linux Security Update for freeradius

[503926](#) Alpine Linux Security Update for freeradius

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report