



CVE-2019-13456

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

Summary

CVE	CVE-2019-13456
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-03 20:15:00 UTC
Updated	2022-01-01 20:06:00 UTC
Description	In FreeRADIUS 3.0 through 3.0.19, on average 1 in every 2048 EAP-pwd handshakes fails because the password element

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeradius	Freeradius	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference
[security-announce] openSUSE-SU-2020:0553-1: moderate: Security update f
Releases
EAP-pwd: fix side-channel leak where 1 in 2048 handshakes fail · FreeRADIUS/freeradius-server@3ea2a5a · GitHub
Dragonblood: Analysing WPA3's Dragonfly Handshake
1737663 – (CVE-2019-13456) CVE-2019-13456 freeradius: eap-pwd: Information leak due to aborting when needing more than 10 iterations
CVE Program record

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159666](#) Oracle Enterprise Linux Security Update for freeradius:3.0 (ELSA-2020-1672)

[377276](#) Alibaba Cloud Linux Security Update for freeradius (ALINUX2-SA-2020:0148)

[750693](#) SUSE Enterprise Linux Security Update for freeradius-server (SUSE-SU-2020:2391-1)

© [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](#)