



CVE-2015-4680

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

Summary

CVE	CVE-2015-4680
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-05 17:59:00 UTC
Updated	2018-10-09 19:57:00 UTC
Description	FreeRADIUS 2.2.x before 2.2.8 and 3.0.x before 3.0.9 does not properly check revocation of intermediate CA certificates.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeradius	Freeradius	2.2.0	All	All	All
Application	Freeradius	Freeradius	2.2.1	All	All	All
Application	Freeradius	Freeradius	2.2.2	All	All	All
Application	Freeradius	Freeradius	2.2.3	All	All	All
Application	Freeradius	Freeradius	2.2.4	All	All	All
Application	Freeradius	Freeradius	2.2.5	All	All	All
Application	Freeradius	Freeradius	2.2.6	All	All	All
Application	Freeradius	Freeradius	2.2.7	All	All	All
Application	Freeradius	Freeradius	3.0.0	All	All	All
Application	Freeradius	Freeradius	3.0.1	All	All	All
Application	Freeradius	Freeradius	3.0.2	All	All	All
Application	Freeradius	Freeradius	3.0.3	All	All	All
Application	Freeradius	Freeradius	3.0.4	All	All	All
Application	Freeradius	Freeradius	3.0.5	All	All	All
Application	Freeradius	Freeradius	3.0.6	All	All	All
Application	Freeradius	Freeradius	3.0.7	All	All	All
Application	Freeradius	Freeradius	3.0.8	All	All	All

Application	Freeradius	Freeradius	2.2.0	All	All	All
Application	Freeradius	Freeradius	2.2.1	All	All	All
Application	Freeradius	Freeradius	2.2.2	All	All	All
Application	Freeradius	Freeradius	2.2.3	All	All	All
Application	Freeradius	Freeradius	2.2.4	All	All	All
Application	Freeradius	Freeradius	2.2.5	All	All	All
Application	Freeradius	Freeradius	2.2.6	All	All	All
Application	Freeradius	Freeradius	2.2.7	All	All	All
Application	Freeradius	Freeradius	3.0.0	All	All	All
Application	Freeradius	Freeradius	3.0.1	All	All	All
Application	Freeradius	Freeradius	3.0.2	All	All	All
Application	Freeradius	Freeradius	3.0.3	All	All	All
Application	Freeradius	Freeradius	3.0.4	All	All	All
Application	Freeradius	Freeradius	3.0.5	All	All	All
Application	Freeradius	Freeradius	3.0.6	All	All	All
Application	Freeradius	Freeradius	3.0.7	All	All	All
Application	Freeradius	Freeradius	3.0.8	All	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Server	12	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp2	All	All

References						
Reference					Source	Link
FreeRADIUS Certificate Validation Code Fails to Check for Revoked Intermediate CA Credentials - SecurityTracker					SECTrack	www.sectrack.com
[security-announce] SUSE-SU-2017:0102-1: important: Security update for					SUSE	lists.opensuse.org
1234975 – (CVE-2015-4680) CVE-2015-4680 freeradius: insufficient CRL application					CONFIRM	bugzilla.mozilla.org
Malformed Request					BID	www.securityfocus.com
SecurityFocus					BUGTRAQ	www.securityfocus.com
oCERT.org - oCERT Advisories					MISC	www.ocert.org

FreeRADIUS Insufficient CRL Application ≈ Packet Storm	MISC	packetst
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.
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](#)