CVE-2011-2701

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-2701
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-08-04 02:45:32 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The ocsp_check function in rlm_eap_tls.c in FreeRADIUS 2.1.11, when OCSP is enabled, does not properly parse replies f

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeradius	Freeradius	2.1.11	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
FreeRADIUS 2.1.11 Multiple Vulns - CXSecurity.com	af854a3a-2127-422b-91a
Security Alerts - Secunia	af854a3a-2127-422b-91a
FreeRADIUS Lets Remote Users Bypass OCSP Certificate Validation Using Expired Certificates - SecurityTracker	af854a3a-2127-422b-91a
SecurityFocus	af854a3a-2127-422b-91a
IBM X-Force Exchange	af854a3a-2127-422b-91a
724815 – (CVE-2011-2701) CVE-2011-2701 freeradius: OCSP does not verify status of certificates	af854a3a-2127-422b-91a
oss-security - CVE request: vulnerability in FreeRADIUS (OCSP)	af854a3a-2127-422b-91a
oss-security - Re: CVE request: vulnerability in FreeRADIUS (OCSP)	af854a3a-2127-422b-91a
Security Advisory FreeRADIUS 2.1.11 - DFN-CERT	af854a3a-2127-422b-91a
oss-security - Re: CVE request: vulnerability in FreeRADIUS (OCSP)	af854a3a-2127-422b-91a
FreeRADIUS Revoked Certificate Authentication Bypass Vulnerability	af854a3a-2127-422b-91a
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.