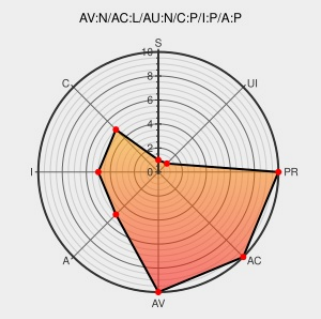
CVE-2005-1455

Published on: 05/19/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1455

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Freeradius from Freeradius contain the following vulnerability:

Buffer overflow in the sql_escape_func function in the SQL module for FreeRADIUS 1.0.2 and earlier allows remote attackers to cause a denial of service (crash).

CVE-2005-1455 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Announcement	web.archive.org, text/html, Inactive Link, Not Archived	SUSE SUSE-SR:2005:014
Gentoo Linux Documentation -- FreeRADIUS: SQL injection and Denial of Service vulnerability	Patch, www.gentoo.org, text/html	GENTOO GLSA-200505-13
rhn.redhat.com | Red Hat Support	www.redhat.com, text/html	REDHAT RHSA-2005:524
FreeRADIUS -- Security Contacts and notifications	www.freeradius.org, text/xml	CONFIRM www.freeradius.org/security.html
Full-Disclosure: [Full-disclosure] ERRATA: [GLSA 200505-13] FreeRADIUS: SQL injection and Denial of Service vulnerability	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20050520 ERRATA: [GLSA 200505-13] FreeRADIUS: SQL injection and Denial of Service vulnerability

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF freeradius-sqlescapefunc-bo(20450)
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:9579
SecurityTracker.com Archives - FreeBSD 'rlm_sql.c' Contains SQL Injection and Buffer Overflow Bugs	www.securitytracker.com text/html	SECTRACK 1013909
FreeRadius RLM_SQL.C Buffer Overflow Vulnerability	Patch cve.report (archive) text/html	BID 13541

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freeradius	Freeradius	1.0.2	All	All	All
Application	Freeradius	Freeradius	1.0.2	All	All	All

cpe:2.3:a:freeradius:freeradius:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→