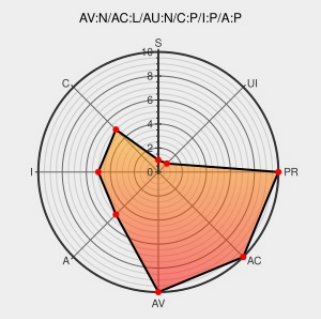
CVE-2006-1354

Published on: 03/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1354

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



Certain versions of Freeradius from Freeradius contain the following vulnerability:

Unspecified vulnerability in FreeRADIUS 1.0.0 up to 1.1.0 allows remote attackers to bypass authentication or cause a denial of service (server crash) via "Insufficient input validation" in the EAP-MSCHAPv2 state machine module.

CVE-2006-1354 has been assigned by cve@mitre.org 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
SGI Advanced Linux Environment 3 Multiple Updates - Advisories - Secunia	web.archive.org text/html	SECUNIA 19811
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: freeradius authentication bypass (SUSE-SA:2006:019)	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:019
Debian -- Security Information -- DSA-1089-1 freeradius	www.debian.org Depreciated Link text/html	DEBIAN DSA-1089
No Description Provided	patches.sgi.com Inactive Link Not Archived	SGI 20060404-01-U
FreeRADIUS EAP-MSCHAPv2 Authentication Bypass Vulnerability - Advisories - Secunia	Patch Vendor Advisory	SECUNIA 19300

	web.archive.org text/html	
rhn.redhat.com | Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2006:0271
Debian update for freeradius - Advisories - Secunia	web.archive.org text/html	SECUNIA 20461
Gentoo update for freeradius - Advisories - Secunia	web.archive.org text/html	SECUNIA 19527
FreeRADIUS EAP-MSCHAPv2 Authentication Bypass Vulnerability	cve.report (archive) text/html	BID 17171
SUSE update for freeradius - Advisories - Secunia	web.archive.org text/html	SECUNIA 19405
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:060
FreeRADIUS -- Security Contacts and notifications	www.freeradius.org text/xml	CONFIRM www.freeradius.org/security.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF freeradius-eap-mschapv2-auth-bypass(25352)
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2006-0020
Red Hat update for freeradius - Advisories - Secunia	web.archive.org text/html	SECUNIA 19518
Gentoo Linux Documentation -- FreeRADIUS: Authentication bypass in EAP-MSCHAPv2 module	www.gentoo.org text/html	GENTOO GLSA-200604-03
FreeRADIUS Input Validation Error in EAP-MSCHAPv2 Module May Let Remote Users Bypass Authentication - SecurityTracker	securitytracker.com text/html	SECTRACK 1015795
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10156
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-1016

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	1.0.0	All	All	All
Application	Freeradius	Freeradius	1.0.1	All	All	All
Application	Freeradius	Freeradius	1.0.2	All	All	All
Application	Freeradius	Freeradius	1.0.3	All	All	All

Application	Freeradius	Freeradius	1.0.3	All	All	All
Application	Freeradius	Freeradius	1.0.4	All	All	All
Application	Freeradius	Freeradius	1.0.5	All	All	All
Application	Freeradius	Freeradius	1.1.0	All	All	All
Application	Freeradius	Freeradius	1.0.0	All	All	All
Application	Freeradius	Freeradius	1.0.1	All	All	All
Application	Freeradius	Freeradius	1.0.2	All	All	All
Application	Freeradius	Freeradius	1.0.3	All	All	All
Application	Freeradius	Freeradius	1.0.4	All	All	All
Application	Freeradius	Freeradius	1.0.5	All	All	All
Application	Freeradius	Freeradius	1.1.0	All	All	All

cpe:2.3:a:freeradius:freeradius:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.1:*:*:*:*:*:*:*:

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

cpe:2.3:a:freeradius:freeradius:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.1:*:*:*:*:*:*:*:

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

cpe:2.3:a:freeradius:freeradius:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:freeradius:freeradius:1.1.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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