



CVE-2001-1376

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

Summary

CVE	CVE-2001-1376
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-03-04 05:00:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Buffer overflow in digest calculation function of multiple RADIUS implementations allows remote attackers to cause a denial of service (DoS) by sending a large number of requests to the server.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ascend	Radius	1.16	All	All	All
Application	Ascend	Radius	1.16	All	All	All
Application	Freeradius	Freeradius	0.2	All	All	All
Application	Freeradius	Freeradius	0.3	All	All	All
Application	Freeradius	Freeradius	0.2	All	All	All
Application	Freeradius	Freeradius	0.3	All	All	All
Application	Gnu	Radius	0.92.1	All	All	All
Application	Gnu	Radius	0.93	All	All	All
Application	Gnu	Radius	0.94	All	All	All
Application	Gnu	Radius	0.95	All	All	All
Application	Gnu	Radius	0.92.1	All	All	All
Application	Gnu	Radius	0.93	All	All	All
Application	Gnu	Radius	0.94	All	All	All
Application	Gnu	Radius	0.95	All	All	All
Application	Icradius	Icradius	0.14	All	All	All
Application	Icradius	Icradius	0.15	All	All	All
Application	Icradius	Icradius	0.16	All	All	All

Application	Icradius	Icradius	0.17	All	All	All
Application	Icradius	Icradius	0.17b	All	All	All
Application	Icradius	Icradius	0.18	All	All	All
Application	Icradius	Icradius	0.18.1	All	All	All
Application	Icradius	Icradius	0.14	All	All	All
Application	Icradius	Icradius	0.15	All	All	All
Application	Icradius	Icradius	0.16	All	All	All
Application	Icradius	Icradius	0.17	All	All	All
Application	Icradius	Icradius	0.17b	All	All	All
Application	Icradius	Icradius	0.18	All	All	All
Application	Icradius	Icradius	0.18.1	All	All	All
Application	Livingston	Radius	2.0	All	All	All
Application	Livingston	Radius	2.0.1	All	All	All
Application	Livingston	Radius	2.1	All	All	All
Application	Livingston	Radius	2.0	All	All	All
Application	Livingston	Radius	2.0.1	All	All	All
Application	Livingston	Radius	2.1	All	All	All
Application	Lucent	Radius	2.0	All	All	All
Application	Lucent	Radius	2.0.1	All	All	All
Application	Lucent	Radius	2.1	All	All	All
Application	Lucent	Radius	2.0	All	All	All
Application	Lucent	Radius	2.0.1	All	All	All
Application	Lucent	Radius	2.1	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.1	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.2	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.3	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.4	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.5	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6_0	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.1	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.2	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.3	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.4	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6.5	All	All	All
Application	Miquel Van Smoorenborg Cistron	Radius	1.6_0	All	All	All

Application	Openradius	Openradius	0.8	All	All	All
Application	Openradius	Openradius	0.9	All	All	All
Application	Openradius	Openradius	0.9.1	All	All	All
Application	Openradius	Openradius	0.9.2	All	All	All
Application	Openradius	Openradius	0.9.3	All	All	All
Application	Openradius	Openradius	0.8	All	All	All
Application	Openradius	Openradius	0.9	All	All	All
Application	Openradius	Openradius	0.9.1	All	All	All
Application	Openradius	Openradius	0.9.2	All	All	All
Application	Openradius	Openradius	0.9.3	All	All	All
Application	Radiusclient	Radiusclient	0.3.1	All	All	All
Application	Radiusclient	Radiusclient	0.3.1	All	All	All
Application	Xtradius	Xtradius	1.1_pre1	All	All	All
Application	Xtradius	Xtradius	1.1_pre1	All	All	All
Application	Yard Radius	Yard Radius	1.0.17	All	All	All
Application	Yard Radius	Yard Radius	1.0.18	All	All	All
Application	Yard Radius	Yard Radius	1.0.19	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre13	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre14	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre15	All	All	All
Application	Yard Radius	Yard Radius	1.0.17	All	All	All
Application	Yard Radius	Yard Radius	1.0.18	All	All	All
Application	Yard Radius	Yard Radius	1.0.19	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre13	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre14	All	All	All
Application	Yard Radius	Yard Radius	1.0_pre15	All	All	All
Application	Yard Radius Project	Yard Radius	1.0.16	All	All	All
Application	Yard Radius Project	Yard Radius	1.0.16	All	All	All

References

Reference

'SECURITY.NNOV: few vulnerabilities in multiple RADIUS implementations' - MARC

SecurityFocus home mailing list: BugTraq

redhat.com | Red Hat Support

Multiple Vendor RADIUS Digest Calculation Buffer Overflow Vulnerability

Home - Conectiva

IBM X-Force Exchange

Neohapsis Archives - SuSE Security Discussion - [suse-security] SuSE Security Announcement: radiusd-cistron (SuSE-SA:2002:013) - From I

CERT Advisory CA-2002-06 Vulnerabilities in Various Implementations of the RADIUS Protocol

CERT/CC Vulnerability Note VU#589523

CVE Program record

NVD vulnerability detail

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)