



CVE-2001-1081

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

Summary

CVE	CVE-2001-1081
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-07-06 04:00:00 UTC
Updated	2008-09-05 20:25:00 UTC
Description	Format string vulnerabilities in Livingston/Lucent RADIUS before 2.1.va.1 may allow local or remote attackers to cause a de

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lucent	Radius	2.1.2	All	All	All
Application	Lucent	Radius	2.1.2	All	All	All
Application	Simon Horns	Radius	2.1_2	All	All	All
Application	Simon Horns	Radius	2.1_2	All	All	All

References

Reference	Source
freshmeat.net: We encountered an error	CONFIRM
[fm-news] 20010713 Newsletter for Friday, July 13th 2001	MLIST
Lucent RADIUS Format String Vulnerability	BID
Neohapsis Archives - VulnWatch - [VulnWatch] Changelog maddness (14 various broken apps) - From rfp@vulnwatch.org	VULNWATCH
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.

© [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](#)