



# CVE-2004-1628

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

## Summary

<b>CVE</b>	CVE-2004-1628
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-10-23 04:00:00 UTC
<b>Updated</b>	2025-04-03 01:03:51 UTC
<b>Description</b>	Format string vulnerability in log.c in rssh before 2.2.2 allows remote authenticated users to execute arbitrary code.

## Risk And Classification

**Primary CVSS:** v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:S/C:C/I:C/A:C

**Problem Types:** CWE-134 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pizzashack	Rssh	All	All	All	All

## Vendor Declared Affected Products

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

## References

Reference	Source	Link
Gentoo Linux Documentation -- rssh: Format string vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.gentoo.org">www.gentoo.org</a>
'rssh: pizzacode security alert' - MARC	af854a3a-2127-422b-91ae-364da2661108	<a href="http://marc.info">marc.info</a>
rssh - restricted shell for scp/sftp	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.pizzashack.org">www.pizzashack.org</a>
Secunia - Advisories - rssh Logging Format String Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="http://secunia.com">secunia.com</a>
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)