



# CVE-2011-1097

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

## Summary

<b>CVE</b>	CVE-2011-1097
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-03-30 22:55:00 UTC
<b>Updated</b>	2023-02-13 01:18:00 UTC
<b>Description</b>	rsync 3.x before 3.0.8, when certain recursion, deletion, and ownership options are used, allows remote rsync servers to ca

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.1	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.2	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.3	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.4	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.5	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.6	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.7	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.1	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.2	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.3	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.4	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.5	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.6	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Rsync</a>	3.0.7	All	All	All

## References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
rsync Incremental Recursion Memory Corruption Vulnerability - Secunia.com	SECUNIA
[SECURITY] Fedora 15 Update: rsync-3.0.8-1.fc15	FEDORA
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:009	SUSE
[SECURITY] Fedora 13 Update: rsync-3.0.8-1.fc13	FEDORA
675036 – (CVE-2011-1097) CVE-2011-1097 rsync: Incremental file-list corruption due to temporary file_extra_cnt increments	CONFIRM
rsync -rcv printing out filenames when content identical	MLIST
Site not found (404)	CONFIRM
[SECURITY] Fedora 14 Update: rsync-3.0.8-1.fc14	FEDORA
'[security bulletin] HPSBMU02752 SSRT100802 rev.1 HP Insight Control Software for Linux (IC-Linux), R' - MARC	HP
gitweb.samba.org - rsync.git/commit	CONFIRM
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Fedora update for rsync - Secunia.com	SECUNIA
access.redhat.com	REDHAT
SecurityTracker: Rsync Checksum Mismatch Error Lets Remote Servers Execute Arbitrary Code	SECTRACK
7936 – Incremental file-list corruption due to temporary file_extra_cnt increments (CVE-2011-1097)	CONFIRM
gitweb.samba.org - rsync.git/commit	MISC
Support / Security / Advisories // MDVSA-2011:066   Mandriva	MANDRIVA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
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](#)**