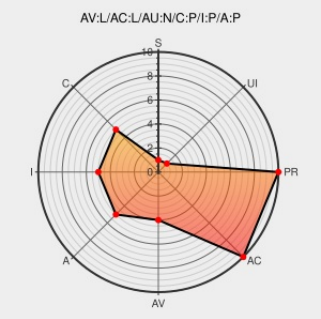
CVE-2005-1064

Published on: 04/10/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1064

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



Certain versions of Filesystem Snapshot Utility from Rsnapshot contain the following vulnerability:

The copy_symlink function in rsnapshot 1.2.0 and 1.1.x before 1.1.7 changes the ownership of files that a symlink points to rather than the symlink itself, which allows local users to obtain access to arbitrary files.

CVE-2005-1064 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Secunia - Advisories - rsnapshot "copy_symlink()" Privilege Escalation Vulnerability	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 14878
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 15420
SecurityTracker.com Archives - rsnapshot copy_symlink() May Let Local Users Gain Elevated Privileges in Certain Situations	Patch, Vendor Advisory, securitytracker.com, text/html	SECTRACK 1013674
rsnapshot	Patch, Vendor Advisory, web.archive.org	CONFIRM www.rsnapshot.org/security/2005/001.html

	text/html Inactive Link Not Archived	
'[Full-disclosure] rsnapshot Security Advisory 001' - MARC	marc.info text/html	FULLDISC 20050410 rsnapshot Security Advisory 001
Gentoo Linux Documentation -- rsnapshot: Local privilege escalation	Patch Vendor Advisory www.gentoo.org text/html	GENTOO GLSA-200504-12

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsnapshot	Filesystem Snapshot Utility	1.0.10	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.1	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.2	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.3	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.4	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.5	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.6	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.2	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.0.10	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.1	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.2	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.3	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.4	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.5	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.1.6	All	All	All
Application	Rsnapshot	Filesystem Snapshot Utility	1.2	All	All	All

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:rsnapshot:filesystem_snapshot_utility:1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→