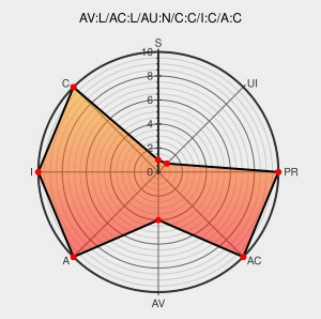
CVE-2005-3345

Published on: 12/28/2005 12:00:00 AM UTC

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

CVE-2005-3345

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



Certain versions of Rssh from Rssh contain the following vulnerability:

rssh 2.0.0 through 2.2.3 allows local users to bypass access restrictions and gain root privileges by using the rssh_chroot_helper command to chroot to an external directory.

CVE-2005-3345 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Gentoo update for rssh - Advisories - Secunia	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 18237
Secunia - Advisories - rssh "chroot" Directory Privilege Escalation Vulnerability	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 18224
#344424 - rssh: local privilege escalation in versions < 2.3.0 (CVE-2005-3345) - Debian Bug report logs	bugs.debian.org, text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=344424
CXSecurity - IDS	securityreason.com, text/html	SREASON 308
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF rssh-chroot-gain-

	text/html	privileges(23854)
rssh security implications	www.pizzashack.org text/html	CONFIRM www.pizzashack.org/rssh/security.shtml
RSSH RSSH_CHROOT_HELPER Local Privilege Escalation Vulnerability	Patch cve.report (archive) text/html	BID 16050
Gentoo Linux Documentation -- rssh: Privilege escalation	Patch Vendor Advisory www.gentoo.org text/html	GENTOO GLSA-200512-15

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rssh	Rssh	2.0	All	All	All
Application	Rssh	Rssh	2.1	All	All	All
Application	Rssh	Rssh	2.2	All	All	All
Application	Rssh	Rssh	2.2.1	All	All	All
Application	Rssh	Rssh	2.2.2	All	All	All
Application	Rssh	Rssh	2.2.3	All	All	All
Application	Rssh	Rssh	2.0	All	All	All
Application	Rssh	Rssh	2.1	All	All	All
Application	Rssh	Rssh	2.2	All	All	All
Application	Rssh	Rssh	2.2.1	All	All	All
Application	Rssh	Rssh	2.2.2	All	All	All
Application	Rssh	Rssh	2.2.3	All	All	All

cpe:2.3:a:rssh:rssh:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:rssh:rssh:2.2.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→