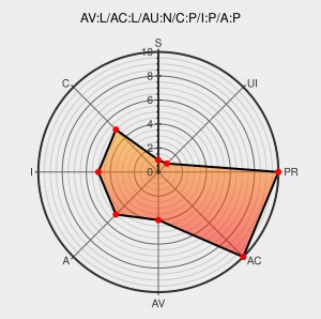
CVE-2005-4620

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4620

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



Certain versions of Winrar from Rarlab contain the following vulnerability:

Buffer overflow in WinRAR 3.50 and earlier allows local users to execute arbitrary code via a long command-line argument. NOTE: because this program executes with the privileges of the invoking user, and because remote programs do not normally have the ability to specify a command-line argument for this program, there may not be a typical attack vector for the issue that crosses privilege boundaries. Therefore this may not be a vulnerability.

CVE-2005-4620 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
	Exploit, www.securityfocus.com, text/x-c, Inactive Link, Not Archived	MISC www.securityfocus.com/data/vulnerabilities/exploits/0xletzdance.c
SecurityFocus	www.securityfocus.com, text/x-c	BUGTRAQ 20060103 Winrar 3.30 Local Buffer Overflow
RARLAB WinRAR Command Line Processing Buffer Overflow Vulnerability	Exploit, cve.report (archive), text/html	BID 15123

WinRAR archiver, a powerful tool to process RAR and ZIP files

www.rarlab.com
text/html

MISC www.rarlab.com/rarnew.htm

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rarlab	Winrar	2.90	All	All	All
Application	Rarlab	Winrar	3.0.0	All	All	All
Application	Rarlab	Winrar	3.10	All	All	All
Application	Rarlab	Winrar	3.10_beta3	All	All	All
Application	Rarlab	Winrar	3.10_beta5	All	All	All
Application	Rarlab	Winrar	3.11	All	All	All
Application	Rarlab	Winrar	3.20	All	All	All
Application	Rarlab	Winrar	3.30	All	All	All
Application	Rarlab	Winrar	3.40	All	All	All
Application	Rarlab	Winrar	3.41	All	All	All
Application	Rarlab	Winrar	3.42	All	All	All
Application	Rarlab	Winrar	3.50	All	All	All
Application	Rarlab	Winrar	2.90	All	All	All
Application	Rarlab	Winrar	3.0.0	All	All	All
Application	Rarlab	Winrar	3.10	All	All	All
Application	Rarlab	Winrar	3.10_beta3	All	All	All
Application	Rarlab	Winrar	3.10_beta5	All	All	All
Application	Rarlab	Winrar	3.11	All	All	All
Application	Rarlab	Winrar	3.20	All	All	All
Application	Rarlab	Winrar	3.30	All	All	All
Application	Rarlab	Winrar	3.40	All	All	All
Application	Rarlab	Winrar	3.41	All	All	All
Application	Rarlab	Winrar	3.42	All	All	All
Application	Rarlab	Winrar	3.50	All	All	All

cpe:2.3:a:rarlab:winrar:2.90:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.20:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.30:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.40:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.41:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.42:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.50:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:2.90:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10_beta3:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.10_beta5:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.20:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.30:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.40:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.41:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.42:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.50:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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