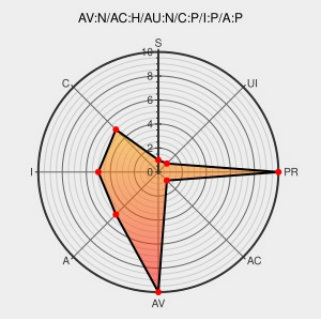
CVE-2005-4474

Published on: 12/21/2005 12:00:00 AM UTC

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

CVE-2005-4474

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



Certain versions of Winrar from Rarlab contain the following vulnerability:

Buffer overflow in the "Add to archive" command in WinRAR 3.51 allows user-assisted attackers to cause a denial of service (crash) and possibly execute arbitrary code by tricking the user into adding a file whose filename contains a non-default code page and non-ANSI characters, as demonstrated using a Chinese filename, possibly due to buffer expansion when using the WideCharToMultiByte API. NOTE: it is not clear whether this problem can be exploited for code execution. If not, then perhaps the user-assisted nature of the attack should exclude the issue from inclusion in CVE.

CVE-2005-4474 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051221 WinRAR - Processing Filename Incorrectly Vulnerability
CXSecurity - IDS	securityreason.com text/html	SREASON 290
RARLAB WinRAR File Name Potential Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 15999

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	3.51	All	All	All
Application	Rarlab	Winrar	3.51	All	All	All

cpe:2.3:a:rarlab:winrar:3.51:*:*:*:*:*:*:*:

cpe:2.3:a:rarlab:winrar:3.51:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→