



CVE-2005-3051

Published on: 09/23/2005 12:00:00 AM UTC

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

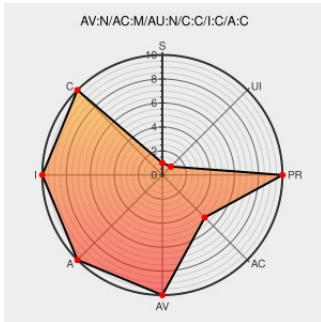
CVE-2005-3051

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **7-zip** from **Igor Pavlov** contain the following vulnerability:

Stack-based buffer overflow in the ARJ plugin (arj.dll) 3.9.2.0 for 7-Zip 3.13, 4.23, and 4.26 BETA, as used in products including Turbo Searcher, allows remote attackers to execute arbitrary code via a large ARJ block.

CVE-2005-3051 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
'Secunia Research: 7-Zip ARJ Archive Handling Buffer Overflow' - MARC	marc.info text/html	BUGTRAQ 20050923 Secunia Research: 7-Zip ARJ Archive Handling Buffer Overflow
Turbo Searcher Buffer Overflow in 'arj.dll' Component Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	SECTRACK 1017261
7-Zip ARJ File Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 14925
About Secunia Research Flexera	Vendor Advisory secunia.com Deprecated Link text/plain	MISC secunia.com/secunia_research/2005-45/advisory/
Knownsoft Turbo Searcher ARJ File Handling Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 21208

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF turbo-searcher-arj-bo(30438)
Secunia - Advisories - 7-Zip ARJ Archive Handling Buffer Overflow	Vendor Advisory web.archive.org text/html	SECUNIA 16664
Turbo Searcher arj.dll Buffer Overflow Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 23004
[vuln.sg] Turbo Searcher 7-Zip ARJ Plugin Buffer Overflow Vulnerability	www.vuln.sg text/html	MISC www.vuln.sg/turbosearcher330-en.html
Webmail- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-4603

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 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	Igor Pavlov	7-zip	3.13	All	All	All
Application	Igor Pavlov	7-zip	4.23	All	All	All
Application	Igor Pavlov	7-zip	4.26_beta	All	All	All
Application	Igor Pavlov	7-zip	3.13	All	All	All
Application	Igor Pavlov	7-zip	4.23	All	All	All
Application	Igor Pavlov	7-zip	4.26_beta	All	All	All

cpe:2.3:a:igor_pavlov:7-zip:3.13:****:*:*:

cpe:2.3:a:igor_pavlov:7-zip:4.23:****:*:*:

cpe:2.3:a:igor_pavlov:7-zip:4.26_beta:****:*:*:

cpe:2.3:a:igor_pavlov:7-zip:3.13:****:*:*:

cpe:2.3:a:igor_pavlov:7-zip:4.23:****:*:*:

cpe:2.3:a:igor_pavlov:7-zip:4.26_beta:****:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)