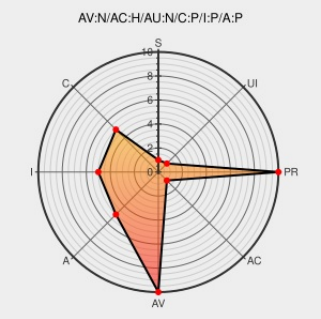
CVE-2006-1513

Published on: 04/25/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1513

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



Certain versions of Abc2ps from Abc2ps contain the following vulnerability:

Multiple buffer overflows in abc2ps before 1.3.3 allow user-assisted attackers to execute arbitrary code via crafted ABC music files.

CVE-2006-1513 has been assigned by security@debian.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
ABC2PS ABC Music Files Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 17689
Debian update for abc2ps - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 19807
About Secunia Research | Flexera	Vendor Advisory web.archive.org text/html	SECUNIA 19787
Debian -- Security Information -- DSA-1041-1 abc2ps	Patch Vendor Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-1041

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-1511
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF abc2ps-abc-bo(26043)

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	Abc2ps	Abc2ps	1.2.2e3	All	All	All
Application	Abc2ps	Abc2ps	1.2.2e4	All	All	All
Application	Abc2ps	Abc2ps	1.2.5	All	All	All
Application	Abc2ps	Abc2ps	1.3.0	All	All	All
Application	Abc2ps	Abc2ps	1.2.2e3	All	All	All
Application	Abc2ps	Abc2ps	1.2.2e4	All	All	All
Application	Abc2ps	Abc2ps	1.2.5	All	All	All
Application	Abc2ps	Abc2ps	1.3.0	All	All	All

cpe:2.3:a:abc2ps:abc2ps:1.2.2e3:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.2.2e4:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.2.2e3:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.2.2e4:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:abc2ps:abc2ps:1.3.0:*:*:*:*:*:*:*:

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 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