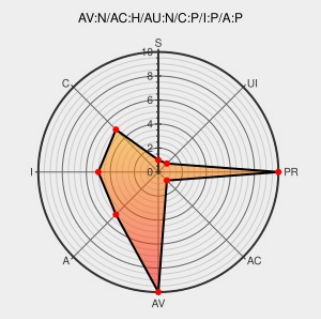
CVE-2005-3376

Published on: 10/29/2005 12:00:00 AM UTC

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

CVE-2005-3376

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



Certain versions of Kaspersky Anti-virus from Kaspersky Lab contain the following vulnerability:

Multiple interpretation error in Kaspersky 5.0.372 allows remote attackers to bypass virus scanning via a file such as BAT, HTML, and EML with an "MZ" magic byte sequence which is normally associated with EXE, which causes the file to be treated as a safe type that could still be executed as a dangerous file type by applications on the end system, as demonstrated by a "triple headed" program that contains EXE, EML, and HTML content, aka the "magic byte bug."

CVE-2005-3376 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
'Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability through' - MARC	marc.info text/html	BUGTRAQ 20051025 Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability through
404 Not Found | AppleElf	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.securityelf.org/magicbyteadv.html
Update for magic byte bug	web.archive.org text/html Inactive Link Not Archived	MISC www.securityelf.org/updmagic.html

Multiple Vendor Anti-Virus Magic Byte Detection Evasion Vulnerability	cve.report (archive) text/html	BID 15189
404 Not Found | AppleElf	web.archive.org text/html Inactive Link Not Archived	MISC www.securityelf.org/magicbyte.html

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	Kaspersky Lab	Kaspersky Anti-virus	5.0.372	All	All	All
Application	Kaspersky Lab	Kaspersky Anti-virus	5.0.372	All	All	All

cpe:2.3:a:kaspersky_lab:kaspersky_anti-virus:5.0.372:*:*:*:*:*:*:*:

cpe:2.3:a:kaspersky_lab:kaspersky_anti-virus:5.0.372:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→