



CVE-2005-3375

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2005-3375
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-30 14:34:00 UTC
Updated	2016-10-18 03:34:00 UTC
Description	Multiple interpretation error in Ikarus demo version allows remote attackers to bypass virus scanning via a file such as BAT,

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ikarus	Ikarus Antivirus	All	All	All	All
Application	Ikarus	Ikarus Antivirus	All	All	All	All

References

Reference	Source	Link	Tags
'Multiple Vendor Anti-Virus Software Detection Evasion Vulnerability through' - MARC	BUGTRAQ	marc.info	
404 Not Found AppleElf	MISC	www.securityelf.org	Vendor Advis
Update for magic byte bug	MISC	www.securityelf.org	
Multiple Vendor Anti-Virus Magic Byte Detection Evasion Vulnerability	BID	www.securityfocus.com	
404 Not Found AppleElf	MISC	www.securityelf.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)