



CVE-2005-3142

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2005-3142
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-05 21:02:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	Heap-based buffer overflow in Kaspersky Antivirus (KAV) 5.0 and Kaspersky Personal Security Suite 1.1 allows remote att

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaspersky Lab	Kaspersky Anti-virus	5.0	All	windows_file_servers	All
Application	Kaspersky Lab	Kaspersky Anti-virus	5.0	All	windows_workstations	All
Application	Kaspersky Lab	Kaspersky Anti-virus	5.0	All	windows_file_servers	All
Application	Kaspersky Lab	Kaspersky Anti-virus	5.0	All	windows_workstations	All
Application	Kaspersky Lab	Kaspersky Anti-virus Personal	5.0	All	All	All
Application	Kaspersky Lab	Kaspersky Anti-virus Personal	5.0	All	All	All
Application	Kaspersky Lab	Kaspersky Anti-virus Personal Pro	5.0	All	All	All
Application	Kaspersky Lab	Kaspersky Anti-virus Personal Pro	5.0	All	All	All
Application	Kaspersky Lab	Kaspersky Personal Security Suite	1.1	All	All	All
Application	Kaspersky Lab	Kaspersky Personal Security Suite	1.1	All	All	All

References

Reference

[Kaspersky Antivirus Remote Heap Overflow - CXSecurity.com](#)

['Kaspersky Antivirus Remote Heap Overflow' - MARC](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[rem0te.com](#)

company information

Secunia - Advisories - Kaspersky Anti-Virus CAB Archive Handling Buffer Overflow

IBM X-Force Exchange

20051003 Kaspersky Antivirus Library Remote Heap Overflow

SecurityTracker.com Archives - Kaspersky Anti-Virus Library Buffer Overflow in Processing CAB Files Lets Remote Users Execute Arbitrary C

19850

Kaspersky Anti-Virus Library CAB Record Remote Heap Overflow Vulnerability

CVE Program record

NVD vulnerability detail



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](#)