



CVE-2009-4114

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

Summary

CVE	CVE-2009-4114
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-11-30 21:30:00 UTC
Updated	2018-10-10 19:48:00 UTC
Description	kl1.sys in Kaspersky Anti-Virus 2010 9.0.0.463, and possibly other versions before 9.0.0.736, does not properly validate inp

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaspersky	Kaspersky Anti-virus	9.0.0.463	All	All	All
Application	Kaspersky	Kaspersky Anti-virus	9.0.0.463	All	All	All

References

Reference	Source
60207	OSVDB
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEL
SecurityFocus	BUGTI
404 Not Found	MISC
SecurityTracker.com Archives - Kaspersky Anti-Virus 'kl1.sys' IOCTL Error Lets Local Users Deny Service	SECTI
IBM X-Force Exchange	XF
Kaspersky Anti-Virus 'kl1.sys' Driver Local Privilege Escalation Vulnerability	BID
Kaspersky Anti-Virus 2010 Denial of Service and Privilege Escalation - Secunia Advisories - Vulnerability Information - Secunia.com	SECUI
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)