



CVE-2014-9643

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

Summary

CVE	CVE-2014-9643
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-06 15:59:00 UTC
Updated	2015-02-09 16:09:00 UTC
Description	K7Sentry.sys in K7 Computing Ultimate Security, Anti-Virus Plus, and Total Security before 14.2.0.253 allows local users to

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	K7computing	Anti-virus Plus	All	All	All	All
Application	K7computing	K7sentry.sys	All	All	All	All
Application	K7computing	Total Security	All	All	All	All
Application	K7computing	Ultimate Security	All	All	All	All

References

Reference	Source
Analysis Of An Interesting Windows Kernel Change Mitigating Vulnerabilities In Some Security Products GreyHatHacker.NET	MISC
K7 Computing Multiple Products Arbitrary Write Privilege Escalation	EXPLOIT-D
K7 Computing 14.2.0.240 Privilege Escalation ≈ Packet Storm	MISC
113007	OSVDB
CVE Program record	CVE.ORG
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](#).

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