



CVE-2007-1281

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

Summary

CVE	CVE-2007-1281
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-06 01:19:00 UTC
Updated	2017-07-29 01:30:00 UTC
Description	Kaspersky AntiVirus Engine 6.0.1.411 for Windows and 5.5-10 for Linux allows remote attackers to cause a denial of service

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 Antivirus Engine	5.5.10	All	All	All
Application	Kaspersky Lab	Kaspersky Antivirus Engine	6.0.1.411	All	All	All
Application	Kaspersky Lab	Kaspersky Antivirus Engine	5.5.10	All	All	All
Application	Kaspersky Lab	Kaspersky Antivirus Engine	6.0.1.411	All	All	All
Operating System	Linux	Linux Kernel	All	All	ia32_64-bit	All
Operating System	Linux	Linux Kernel	All	All	ia32_64-bit	All
Operating System	Microsoft	All Windows	abstract_cpe	All	All	All
Operating System	Microsoft	All Windows	abstract_cpe	All	All	All

References

Reference	Source	Link
Kaspersky Anti-Virus Engine UPX Processing Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
Kaspersky AntiVirus UPX File Decompression Remote Denial of Service Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Kaspersky Anti-Virus Error in Processing UPX Files Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com
20070302 Kaspersky AntiVirus UPX File Decompression DoS Vulnerability	IDEFENSE	labs.iddefense.com

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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