



# CVE-2005-3922

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

## Summary

<b>CVE</b>	CVE-2005-3922
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-30 11:03:00 UTC
<b>Updated</b>	2018-10-19 15:39:00 UTC
<b>Description</b>	Heap-based buffer overflow in pskcmp.dll in Panda Software Antivirus library allows remote attackers to execute arbitrary c

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Panda</a>	<a href="#">Panda Activescan</a>	5.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Activescan</a>	5.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Antivirus</a>	2.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Antivirus</a>	2.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Antivirus Platinum</a>	2.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Antivirus Platinum</a>	2.0	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Businesssecure Antivirus</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Businesssecure Antivirus</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Clientshield With Truprevent Technologies</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Clientshield With Truprevent Technologies</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Enterprisesecure With Truprevent Technologies</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Enterprisesecure With Truprevent Technologies</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Exchangesecure</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Exchangesecure</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Filesecure</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Filesecure</a>	All	All	All	All
Application	<a href="#">Panda</a>	<a href="#">Panda Filesecure With Truprevent Technologies</a>	All	All	All	All

Application	Panda	Panda Filesecure With Truprevent Technologies	All	All	All	All
Application	Panda	Panda Gatedefender	All	All	All	All
Application	Panda	Panda Gatedefender	All	All	All	All
Application	Panda	Panda Isa Secure	All	All	All	All
Application	Panda	Panda Isa Secure	All	All	All	All
Application	Panda	Panda Panda Enterprisesecure Antivirus	All	All	All	All
Application	Panda	Panda Panda Enterprisesecure Antivirus	All	All	All	All
Application	Panda	Panda Platinum 2006 Internet Security	All	All	All	All
Application	Panda	Panda Platinum 2006 Internet Security	All	All	All	All
Application	Panda	Panda Security	3.0	All	All	All
Application	Panda	Panda Security	3.0	All	All	All
Application	Panda	Panda Titanium	All	All	All	All
Application	Panda	Panda Titanium	All	All	All	All
Application	Panda	Panda Titanium 2005 Antivirus	All	All	All	All
Application	Panda	Panda Titanium 2005 Antivirus	All	All	All	All
Application	Panda	Panda Titanium 2006 Antivirus Antispyware	All	All	All	All
Application	Panda	Panda Titanium 2006 Antivirus Antispyware	All	All	All	All
Application	Panda	Panda Titanium 2006 Antivirus Antispyware	All	All	All	All
Application	Panda	Panda Truprevent Personal	2005	All	All	All
Application	Panda	Panda Truprevent Personal	2006	All	All	All
Application	Panda	Panda Truprevent Personal	2005	All	All	All
Application	Panda	Panda Truprevent Personal	2006	All	All	All
Application	Panda	Panda Webadmin	All	All	All	All
Application	Panda	Panda Webadmin	All	All	All	All

## References

### Reference

SecurityFocus

rem0te.com

21256

SecurityTracker.com Archives - Panda Antivirus Heap Overflow in Processing ZOO Archives May Let Remote Users Execute Arbitrary Code

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM X-Force Exchange

Secunia - Advisories - Panda Antivirus ZOO Archive Decompression Buffer Overflow

Panda Software Antivirus Library ZOO Archive 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](#)