



CVE-2008-3865

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

Summary

CVE	CVE-2008-3865
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-21 20:30:00 UTC
Updated	2018-10-11 20:50:00 UTC
Description	Multiple heap-based buffer overflows in the ApiThread function in the firewall service (aka TmPfw.exe) in Trend Micro Netw

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trend Micro	Internet Security 2007	All	All	All	All
Application	Trend Micro	Internet Security 2007	All	All	All	All
Application	Trend Micro	Internet Security 2008	17.0.1224	All	All	All
Application	Trend Micro	Internet Security 2008	17.0.1224	All	All	All
Application	Trend Micro	Officescan	8.0	sp1	All	All
Application	Trend Micro	Officescan	8.0	sp1	All	All

References

Reference	Source
SecurityReason - Trend Micro Network Security Component Vulnerabilities	SREASON
Trend Micro Internet Security Buffer Overflow Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK
www.trendmicro.com/ftp/documentation/readme/OSCE8.0_SP1_Patch1_CriticalPatch_319...	CONFIRM
Trend Micro OfficeScan Client Firewall Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Trend Micro Internet Security Firewall Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IBM X-Force Exchange	XF
Vulnerabilities - Secunia Research - Vulnerability Intelligence - Secunia.com	MISC

Trend Micro OfficeScan Buffer Overflow Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK
Trend Micro Multiple Products Network Security Component Modules Multiple Vulnerabilities	BID
SecurityFocus	BUGTRAQ
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](#)