



CVE-2007-0602

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

Summary

CVE	CVE-2007-0602
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-30 18:28:00 UTC
Updated	2018-10-16 16:33:00 UTC
Description	Buffer overflow in libvsapi.so in the VSAPI library in Trend Micro VirusWall 3.81 for Linux, as used by IScan.BASE/vscan, a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trend Micro	Viruswall	3.81	All	All	All
Application	Trend Micro	Viruswall	3.81	All	All	All

References

Reference	Source
Buffer overflow in VSAPI library of Trend Micro VirusWall 3.81 for Linux - CXSecurity.com	SREA
SecurityFocus	BUGT
Bot Verification	MISC
SecurityTracker.com Archives - InterScan VirusWall Buffer Overflow in 'libvsapi.so' May Let Local Users Gain Elevated Privileges	SECT
[Vulnerability Response] - Segmentation fault in Trend Micro InterScan VirusWall (ISVW) 3.81 for Linux virus scan tool [EN-1034124]	CONF
33043	OSVD
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	UPE
Bot Verification	MISC
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](#).

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