



CVE-2006-6293

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

Summary

CVE	CVE-2006-6293
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-12-05 11:28:00 UTC
Updated	2018-10-17 21:47:00 UTC
Description	Heap-based buffer overflow in FRISK Software F-Prot Antivirus before 4.6.7 allows user-assisted remote attackers to execute

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F-prot	F-prot Antivirus	3.11b	All	All	All
Application	F-prot	F-prot Antivirus	3.12	All	All	All
Application	F-prot	F-prot Antivirus	3.12a	All	All	All
Application	F-prot	F-prot Antivirus	3.12b	All	All	All
Application	F-prot	F-prot Antivirus	3.12c	All	All	All
Application	F-prot	F-prot Antivirus	3.12d	All	All	All
Application	F-prot	F-prot Antivirus	3.13	All	All	All
Application	F-prot	F-prot Antivirus	3.13a	All	All	All
Application	F-prot	F-prot Antivirus	3.14	All	All	All
Application	F-prot	F-prot Antivirus	3.14a	All	All	All
Application	F-prot	F-prot Antivirus	3.14b	All	All	All
Application	F-prot	F-prot Antivirus	3.14c	All	All	All
Application	F-prot	F-prot Antivirus	3.14d	All	All	All
Application	F-prot	F-prot Antivirus	3.14e	All	All	All
Application	F-prot	F-prot Antivirus	3.15	All	All	All
Application	F-prot	F-prot Antivirus	3.15a	All	All	All
Application	F-prot	F-prot Antivirus	3.15b	All	All	All

Application	F-prot	F-prot Antivirus	3.16	All	All	All
Application	F-prot	F-prot Antivirus	3.16a	All	All	All
Application	F-prot	F-prot Antivirus	3.16b	All	All	All
Application	F-prot	F-prot Antivirus	3.16c	All	All	All
Application	F-prot	F-prot Antivirus	3.16d	All	All	All
Application	F-prot	F-prot Antivirus	3.16e	All	All	All
Application	F-prot	F-prot Antivirus	3.16f	All	All	All
Application	F-prot	F-prot Antivirus	3.11b	All	All	All
Application	F-prot	F-prot Antivirus	3.12	All	All	All
Application	F-prot	F-prot Antivirus	3.12a	All	All	All
Application	F-prot	F-prot Antivirus	3.12b	All	All	All
Application	F-prot	F-prot Antivirus	3.12c	All	All	All
Application	F-prot	F-prot Antivirus	3.12d	All	All	All
Application	F-prot	F-prot Antivirus	3.13	All	All	All
Application	F-prot	F-prot Antivirus	3.13a	All	All	All
Application	F-prot	F-prot Antivirus	3.14	All	All	All
Application	F-prot	F-prot Antivirus	3.14a	All	All	All
Application	F-prot	F-prot Antivirus	3.14b	All	All	All
Application	F-prot	F-prot Antivirus	3.14c	All	All	All
Application	F-prot	F-prot Antivirus	3.14d	All	All	All
Application	F-prot	F-prot Antivirus	3.14e	All	All	All
Application	F-prot	F-prot Antivirus	3.15	All	All	All
Application	F-prot	F-prot Antivirus	3.15a	All	All	All
Application	F-prot	F-prot Antivirus	3.15b	All	All	All
Application	F-prot	F-prot Antivirus	3.16	All	All	All
Application	F-prot	F-prot Antivirus	3.16a	All	All	All
Application	F-prot	F-prot Antivirus	3.16b	All	All	All
Application	F-prot	F-prot Antivirus	3.16c	All	All	All
Application	F-prot	F-prot Antivirus	3.16d	All	All	All
Application	F-prot	F-prot Antivirus	3.16e	All	All	All
Application	F-prot	F-prot Antivirus	3.16f	All	All	All
Application	F-prot	F-prot Antivirus	All	All	All	All

References

Reference

Wang, J., G. Li, and J. Wang. 2019. "A Novel F-prot Antivirus." *Journal of Computer Science* 10(1): 1-10.

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Full-disclosure] F-Prot Antivirus for Unix: heap overflow and Denial of Service

SecurityTracker.com Archives - F-Prot Antivirus CHM File Buffer Overflow and ACE Archive Infinite Loop Lets Remote Users Execute Arbitrar

GLEG Ltd. - Information Security Company

SecurityFocus

F-Prot AntiVirus 4.6.6 - CHM Heap Overflow (PoC) - Linux dos Exploit

F-PROT Antivirus EOL Announcement

404 Not Found

F-PROT Antivirus CHM File Heap Buffer Overflow Vulnerability

Gentoo Linux Documentation -- F-PROT Antivirus: Multiple vulnerabilities

30406

F-PROT Antivirus ACE and CHM File Handling Vulnerabilities - Advisories - Secunia

Gentoo update for f-prot - Advisories - Secunia

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](#)