



# CVE-2007-2966

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-2966
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-05-31 23:30:00 UTC
<b>Updated</b>	2018-10-16 16:46:00 UTC
<b>Description</b>	Buffer overflow in the LHA decompression component in F-Secure anti-virus products for Microsoft Windows and Linux bef

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F-secure	F-secure Anti-virus	2005	All	All	All
Application	F-secure	F-secure Anti-virus	2006	All	All	All
Application	F-secure	F-secure Anti-virus	2007	All	All	All
Application	F-secure	F-secure Anti-virus	2005	All	All	All
Application	F-secure	F-secure Anti-virus	2006	All	All	All
Application	F-secure	F-secure Anti-virus	2007	All	All	All
Application	F-secure	F-secure Anti-virus	All	All	linux_gateways	All
Application	F-secure	F-secure Anti-virus	All	All	linux_servers	All
Application	F-secure	F-secure Anti-virus	All	All	windows_servers	All
Application	F-secure	F-secure Anti-virus	All	All	workstations	All
Application	F-secure	F-secure Anti-virus	All	All	citrix_servers	All
Application	F-secure	F-secure Anti-virus	All	All	mimesweeper	All
Application	F-secure	F-secure Anti-virus	All	All	ms_exchange	All
Application	F-secure	F-secure Anti-virus Client Security	All	All	All	All
Application	F-secure	F-secure Anti-virus Linux Client Security	All	All	All	All
Application	F-secure	F-secure Anti-virus Linux Server Security	All	All	All	All
Application	F-secure	F-secure Internet Security	2005	All	All	All

Application	F-secure	F-secure Internet Security	2006	All	All	All
Application	F-secure	F-secure Internet Security	2007	All	All	All
Application	F-secure	F-secure Internet Security	2005	All	All	All
Application	F-secure	F-secure Internet Security	2006	All	All	All
Application	F-secure	F-secure Internet Security	2007	All	All	All
Application	F-secure	F-secure Protection Service	All	All	consumers	All
Application	F-secure	Internet Gatekeeper	All	All	linux	All
Application	F-secure	Internet Gatekeeper	All	All	All	All

## References

### Reference

F-Secure Anti-Virus LHA Processing Buffer Overflow Vulnerability

n.runs AG - Security Tools and Security Advisories

SecurityTracker.com Archives - F-Secure Internet Gatekeeper Lets Remote Users Execute Arbitrary Code

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM X-Force Exchange

F-Secure Products LHA Archive Handling Buffer Overflow - Advisories - Secunia

F-Secure Security Bulletin FSC-2007-1

SecurityTracker.com Archives - F-Secure Internet Security Lets Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges

36724

SecurityTracker.com Archives - F-Secure Anti-Virus Lets Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges

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](#)**