



CVE-2006-4331

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

Summary

CVE	CVE-2006-4331
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-24 20:04:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	Multiple off-by-one errors in the IPSec ESP preference parser in Wireshark (formerly Ethereal) 0.99.2 allow remote attacker

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All

References

Reference

Avaya Products Wireshark Multiple Vulnerabilities - Advisories - Secunia

Advisories - Mandriva Linux

Wireshark Multiple Vulnerabilities

Mandriva update for wireshark - Advisories - Secunia

US-CERT Vulnerability Notes

Wireshark: wnpa-sec-2006-02

rPath update for tshark / wireshark - Advisories - Secunia

IBM X-Force Exchange

Repository / Oval Repository

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Support

SecurityTracker.com Archives - Wireshark (Ethereal) Bugs in SCSI, DHCP, and Q.2931 Dissectors Let Remote Users Execute Arbitrary Code

Wireshark Multiple Vulnerabilities - Advisories - Secunia
ASA-2006-227 (RHSA-2006-0658)
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities
Gentoo update for wireshark - Advisories - Secunia
Repository / Oval Repository
Red Hat update for wireshark - 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](#).

Free CVE JSON API [cve.report/api](#)

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