CVE-2006-4333

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-4333
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-24 20:04:00 UTC
Updated	2018-10-17 21:34:00 UTC
Description	The SSCOP dissector in Wireshark (formerly Ethereal) before 0.99.3 allows remote attackers to cause a denial of service (r

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.10.13	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.99	All	All	All
Application	Wireshark	Wireshark	0.99.1	All	All	All
Application	Wireshark	Wireshark	0.99.2	All	All	All
Application	Wireshark	Wireshark	0.10.13	All	All	All
Application	Wireshark	Wireshark	0.10.4	All	All	All
Application	Wireshark	Wireshark	0.99	All	All	All
Application	Wireshark	Wireshark	0.99.1	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

Wireshark: wnpa-sec-2006-02
rPath update for tshark / wireshark - Advisories - Secunia
Debian -- Security Information -- DSA-1171-1 ethereal
Repository / Oval Repository
IBM X-Force Exchange
US-CERT Vulnerability Note VU#696896
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityFocus
Support
[#RPL-597] wireshark in rpl:1 is vulnerable to 4 issues - rPath JIRA
SecurityTracker.com Archives - Wireshark (Ethereal) Bugs in SCSI, DHCP, and Q.2931 Dissectors Let Remote Users Execute Arbitrary Code
Debian update for ethereal - Advisories - Secunia
IBM X-Force Exchange
Wireshark Multiple Vulnerabilities - Advisories - Secunia
ASA-2006-227 (RHSA-2006-0658)
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities
Gentoo update for wireshark - Advisories - Secunia
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 registred 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**