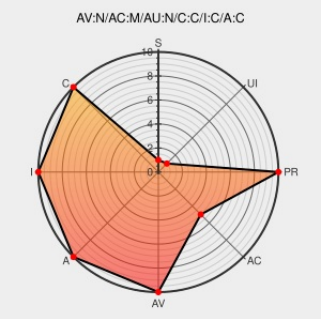
CVE-2011-1591

Published on: 04/29/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:08 AM UTC

CVE-2011-1591

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Stack-based buffer overflow in the DECT dissector in epan/dissectors/packet-dect.c in Wireshark 1.4.x before 1.4.5 allows remote attackers to execute arbitrary code via a crafted .pcap file.

CVE-2011-1591 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Wireshark Denial of Service and Buffer Overflow Vulnerabilities - Secunia.com	web.archive.org text/html	SECUNIA 44172
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF wireshark-dect-bo(66834)
Wireshark · wnpa-sec-2011-06	www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2011-06.html
Wireshark Buffer Overflow in DECT Dissector Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	SECTRACK 1025389
5838 – Buffer overflow in Wireshark 1.4.1	Exploit bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=5838

Support / Security / Advisories / / MDVSA-2011:083 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2011:083
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2011-1106
Wireshark <= 1.4.4 packet-dect.c Stack Buffer Overflow	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 17195
[SECURITY] Fedora 14 Update: wireshark-1.4.6-1.fc14	lists.fedoraproject.org text/html	FEDORA FEDORA-2011-5569
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2011-1022
[SECURITY] Fedora 13 Update: wireshark-1.2.16-1.fc13	lists.fedoraproject.org text/html	FEDORA FEDORA-2011-5529
oss-security - Wireshark 1.2.16 / 1.4.5	openwall.com text/html	MLIST [oss-security] 20110418 Wireshark 1.2.16 / 1.4.5
oss-security - Re: Wireshark 1.2.16 / 1.4.5	openwall.com text/html	MLIST [oss-security] 20110418 Re: Wireshark 1.2.16 / 1.4.5
5836 – possibly exploitable crash	Exploit bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=5836
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 71848
US-CERT Vulnerability Note VU#243670 - Wireshark DECT dissector vulnerability	US Government Resource www.kb.cert.org text/html	CERT-VN VU#243670
Wireshark 1.4.1-1.4.4 SEH Overflow Exploit	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 17185
Security Alerts - Secunia	web.archive.org text/html	SECUNIA 44374
[SECURITY] Fedora 15 Update: wireshark-1.4.6-1.fc15	lists.fedoraproject.org text/html	FEDORA FEDORA-2011-5621
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:15000

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.4.0	All	All	All

Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All

cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
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.

CVE.report and Source URL Uptime Status status.cve.report