CVE-2010-4301

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

Summary

CVE	CVE-2010-4301
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-26 19:00:00 UTC
Updated	2017-09-19 01:31:00 UTC
Description	epan/dissectors/packet-zbee-zcl.c in the ZigBee ZCL dissector in Wireshark 1.4.0 through 1.4.1 allows remote attackers to

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

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	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
5303 – Infinite loop in ZCL Discover Attributes dissection	CONFIRM	bugs.wireshark.org
Attachment 5315 Details for Bug 5303 – Patch to correct ZCL Discover Attributes Response dissector	MISC	bugs.wireshark.org
Wireshark · wnpa-sec-2010-14	CONFIRM	www.wireshark.org
69355	OSVDB	osvdb.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:001	SUSE	lists.opensuse.org
Wireshark Two Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
Wireshark ZigBee ZCL Dissector Infinite Loop Denial of Service Vulnerability	BID	www.securityfocus.cc
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com

SUSE update for multiple packages - Advisories - Community	SECUNIA	secunia.com
Wireshark ZigBee ZCL Dissector Infinite Loop Denial of Service	EXPLOIT-DB	www.exploit-db.com
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	SUSE	lists.opensuse.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
SUSE update for Multiple Packages - Secunia.com	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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