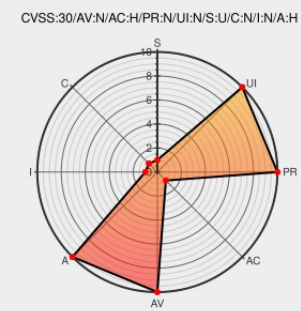
CVE-2016-5351

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5351

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

epan/crypt/airpdcap.c in the IEEE 802.11 dissector in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles the lack of an EAPOL_RSN_KEY, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2016-5351 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3615-1 wireshark	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3615
Wireshark · wnpa-sec-2016-30	Vendor Advisory	CONFIRM www.wireshark.org/security/wnpa-sec-2016-30.html

· IEEE 802.11 dissector crash	www.wireshark.org text/html	
Wireshark Multiple Denial of Service Vulnerabilities	cve.report (archive) text/html	BID 91140
Make sure EAPOL body is big enough for a EAPOL_RSN_KEY. · wireshark/wireshark@9b0b20b · GitHub	github.com text/html	CONFIRM github.com/wireshark/wireshark/commit/9b0b20b8d5f8c9f7839d58ff6c5900f7e19283b4
11585 – Buildbot crash output: fuzz-2015-10-10-13251.pcap	Exploit Issue Tracking bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11585
oss-security - Re: CVE Request: wireshark releases	Mailing List www.openwall.com text/html	MLIST [oss-security] 20160609 Re: CVE Request: wireshark releases
Oracle Solaris Bulletin - July 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html

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	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.10	All	All	All
Application	Wireshark	Wireshark	1.12.11	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All
Application	Wireshark	Wireshark	1.12.5	All	All	All
Application	Wireshark	Wireshark	1.12.6	All	All	All
Application	Wireshark	Wireshark	1.12.7	All	All	All
Application	Wireshark	Wireshark	1.12.8	All	All	All
Application	Wireshark	Wireshark	1.12.9	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All

Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.10	All	All	All
Application	Wireshark	Wireshark	1.12.11	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All
Application	Wireshark	Wireshark	1.12.5	All	All	All
Application	Wireshark	Wireshark	1.12.6	All	All	All
Application	Wireshark	Wireshark	1.12.7	All	All	All
Application	Wireshark	Wireshark	1.12.8	All	All	All
Application	Wireshark	Wireshark	1.12.9	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.11:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.11:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:2.0.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→