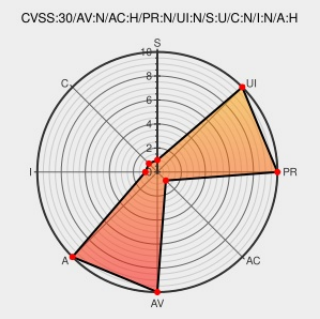
CVE-2016-4083

Published on: 04/25/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:59 PM UTC

CVE-2016-4083

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.3 does not ensure that data is available before array allocation, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2016-4083 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
Wireshark Multiple Dissector Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1035685
code.wireshark Code Review -	code.wireshark.org	CONFIRM code.wireshark.org/review/gitweb?

wireshark.git/commit	text/xml	p=wireshark.git;a=commit;h=66417b17b3570b163a16ca81f71ce5bcb10548d2
Wireshark · wnpa-sec-2016-27 · MS-WSP dissector crash	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2016-27.html
12341 – Buildbot crash output: fuzz-2016-04-12-9951.pcap	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=12341

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	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	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All

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:2.0.0:*:*:*:*:*:*:*

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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