



CVE-2016-6503

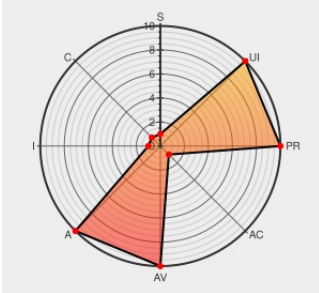
Published on: 08/06/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:34:00 AM UTC

CVE-2016-6503

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Wireshark](#) from [Wireshark](#) contain the following vulnerability:

The CORBA IDL dissectors in Wireshark 2.x before 2.0.5 on 64-bit Windows platforms do not properly interact with Visual C++ compiler options, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2016-6503 has been assigned by [M](#) 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 2.0.0 - 2.0.4 - CORBA IDL Dissectors Denial of Service	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 40196
code.wireshark Code Review -	code.wireshark.org	CONFIRM code.wireshark.org/review/gitweb?

wireshark.git/commit	text/xml	p=wireshark.git;a=commit;h=581a17af40b84ef0c9e7f41ed0795af345b61ce1
Wireshark Dissector/Parser Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTrack 1036480
oss-security - CVE request: Wireshark 2.0.5 and 1.12.13 security releases	Mailing List openwall.com text/html	MLIST [oss-security] 20160728 CVE request: Wireshark 2.0.5 and 1.12.13 security releases
Wireshark CORBA IDL Dissector Denial of Service Vulnerability	cve.report (archive) text/html	BID 92162
Wireshark · wnpa-sec-2016-39 · CORBA IDL dissector crash on 64-bit Windows.	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2016-39.html
12495 – Crash in Corba auto generated files with MSVC2013 Update 5 x64	Issue Tracking bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=12495

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	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	2.0.4	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	2.0.4	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:2.0.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.4:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.0:*:*:*:*:*:						

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:2.0.4:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)