



CVE-2016-2524

Published on: 02/27/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-2524

[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:

epan/dissectors/packet-x509af.c in the X.509AF dissector in Wireshark 2.0.x before 2.0.2 mishandles the algorithm ID, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2016-2524 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 Multiple Dissector/Parser Bugs Let Remote Users Deny Service and Let Local Users Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTrack 1035118

Wireshark: Multiple vulnerabilities (GLSA 201604-05) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201604-05
12002 – Buildbot crash output: fuzz-2016-01-12-29381.pcap	Vendor Advisory bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=12002
Wireshark · wnpa-sec-2016-04 · X.509AF crash	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2016-04.html
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=5a8020a1b6bb73fcb8bb7eb7d53177bc8a9fc703

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	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	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:2.0.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)