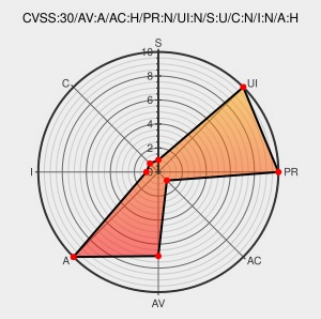
CVE-2015-8740

Published on: 01/03/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8740

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

The dissect_tds7_colmetadata_token function in epan/dissectors/packet-tds.c in the TDS dissector in Wireshark 2.0.x before 2.0.1 does not validate the number of columns, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.

CVE-2015-8740 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_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 vulnerabilities (GLSA 201604-05) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201604-05

Wireshark Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 79382
Bug 11846 – Wireshark stack-based buffer overflow in dissect_tds7_colmetadata_token	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11846
Wireshark Multiple Dissector/Parser Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034551
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=e78093f69f1e95df919bbe644baa06c7e4e720c0
Wireshark · wnpa-sec-2015-58 · TDS dissector crash	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2015-58.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	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→