wnpa-sec-2022-02 · Large loops in multiple dissectors

Summary

Name: Large loops in multiple dissectors

Docid: wnpa-sec-2022-02

Date: February 10, 2022

Affected versions: 3.6.0 to 3.6.1, 3.4.0 to 3.4.11

Fixed versions: 3.6.2, 3.4.12

References:
Wireshark issue 17829 (https://gitlab.com/wireshark/wireshark/-/issues/17829)
Wireshark issue 17842 (https://gitlab.com/wireshark/wireshark/-/issues/17842)
Wireshark issue 17847 (https://gitlab.com/wireshark/wireshark/-/issues/17847)
Wireshark issue 17855 (https://gitlab.com/wireshark/wireshark/-/issues/17855)
Wireshark issue 17891 (https://gitlab.com/wireshark/wireshark/-/issues/17891)
Wireshark issue 17925 (https://gitlab.com/wireshark/wireshark/-/issues/17925)
Wireshark issue 17926 (https://gitlab.com/wireshark/wireshark/-/issues/17926)
Wireshark issue 17931 (https://gitlab.com/wireshark/wireshark/-/issues/17931)
Wireshark issue 17932 (https://gitlab.com/wireshark/wireshark/-/issues/17932)
Wireshark issue 17933 (https://gitlab.com/wireshark/wireshark/-/issues/17933)
CVE-2022-0585 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0585)

Details

Description

Large loops were discovered in multiple dissectors, including AMP, ATN-ULCS and possibly other ASN.1 PER dissectors, BP, GDSDB, OpenFlow v5, P_MUL, SoulSeek, TDS, WBXML, WSP and possibly other WAP dissectors, and ZigBee ZCL. Discovered by Sharon Brizinov.

Impact

It may be possible to make Wireshark consume excessive CPU resources by injecting a malformed packet onto the wire or by convincing someone to read a malformed packet trace file.

Resolution

Upgrade to Wireshark 3.6.2, 3.4.12 or later.

Wireshark and the "fin" logo are registered trademarks. | Twitter (https://twitter.com/wiresharknews) | YouTube (youtube.com/c/sharkFestWiresharkDeveloperandUserConference) | Mastodon (https://ioc.exchange/@wireshark) | Facebook (https://www.facebook.com/SHARKFEST-Wireshark-Network-Analysis-Conference-51502216870/) | Privacy policy (https://sysdig.com/privacy-policy/)

Back to top