| Vulnerability Type(s) | Publish Date | CVSSS | Description & CVE ID | Reference /Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Wireshark** | | | | | |
| ***Wireshark*** | | | | | |
| NA | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record. **CVE-ID:CVE-2018-11356** | https://www.wireshark.org/security/wnpa-sec-2018-29.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=4425716ddba99374749bd033d9bc0f4add2fb973<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14681 | A-Wir-Wires/01-06-18/1 |
| NA | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths. **CVE-ID:CVE-2018-11357** | https://www.wireshark.org/security/wnpa-sec-2018-28.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=ab8a33ef083b9732c89117747a83a905a676faf6<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14678 | A-Wir-Wires/01-06-18/2 |
| NA | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the Q.931 dissector could crash. This was addressed in epan/dissectors/packet-q931.c by avoiding a use-after-free after a malformed packet prevented certain cleanup. **CVE-ID:CVE-2018-11358** | https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=ccb1ac3c8cec47fbbbf2e80ced80644005c65252<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14689<br><br>https://www.wireshark.org/ | A-Wir-Wires/01-06-18/3 |

| Vulnerability Type(s) | Publish Date | CVSSS | Description & CVE ID | Reference /Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | security/wnpa-sec-2018-31.html | |
| NA | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the RRC dissector and other dissectors could crash. This was addressed in epan/proto.c by avoiding a NULL pointer dereference. **CVE-ID:CVE-2018-11359** | https://www.wireshark.org/security/wnpa-sec-2018-33.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=beaebe91b14564fb9f86f0726bab09927872721b<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14703 | A-Wir-Wires/01-06-18/4 |
| NA | 22-05-2018 | 5 | In Wireshark 2.6.0, the IEEE 1905.1a dissector could crash. This was addressed in epan/dissectors/packet-ieee1905.c by making a certain correction to string handling. **CVE-ID:CVE-2018-11354** | https://www.wireshark.org/security/wnpa-sec-2018-26.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=cb517a4a434387e74a2f75ebb106ee3c3893251c<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14647 | A-Wir-Wires/01-06-18/5 |
| Overflow | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the GSM A DTAP dissector could crash. This was addressed in epan/dissectors/packet-gsm_a_dtap.c by fixing an off-by-one error that caused a buffer overflow. **CVE-ID:CVE-2018-11360** | https://www.wireshark.org/security/wnpa-sec-2018-30.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=a55b36c51f83a7b9680824e8ee3a6ce8429ab24b<br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14688 | A-Wir-Wires/01-06-18/6 |
| Overflow | 22-05-2018 | 5 | In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the LDSS dissector could | https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=f177008b04a | A-Wir-Wires/ |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**

| Vulnerability Type(s) | Publish Date | CVSSS | Description & CVE ID | Reference /Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crash. This was addressed in epan/dissectors/packet-ldss.c by avoiding a buffer over-read upon encountering a missing '0' character. **CVE-ID:CVE-2018-11362** | 530640de835ca878892e58b826d58<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14615<br><br>https://www.wireshark.org/security/wnpa-sec-2018-25.html | 01-06-18/7 |
| Overflow | 22-05-2018 | 5 | In Wireshark 2.6.0, the IEEE 802.11 protocol dissector could crash. This was addressed in epan/crypt/dot11decrypt.c by avoiding a buffer overflow during FTE processing in Dot11DecryptTDLSDeriveKey. **CVE-ID:CVE-2018-11361** | https://www.wireshark.org/security/wnpa-sec-2018-32.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=1b52f9929238ce3948ec924ae4f9456b5e9df558<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14686 | A-Wir-Wires/01-06-18/8 |
| Overflow | 22-05-2018 | 5 | In Wireshark 2.6.0, the RTCP dissector could crash. This was addressed in epan/dissectors/packet-rtcp.c by avoiding a buffer overflow for packet status chunks. **CVE-ID:CVE-2018-11355** | https://www.wireshark.org/security/wnpa-sec-2018-27.html<br><br>https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=99d27a5fd2c540f837154aca3b3647f5ccfa0c33<br><br>https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=14673 | A-Wir-Wires/01-06-18/9 |

| CV Scoring Scale (CVSS) | 3-4 | 4-5 | 5-6 | 6-7 | 7-8 | 8-9 | 9-10 |
|---|---|---|---|---|---|---|---|

**Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS- Cross Site Scripting;**