

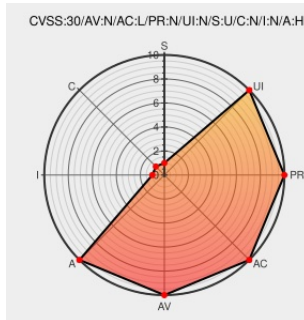


CVE-2017-11411

Published on: 07/18/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:38:00 AM UTC

CVE-2017-11411

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

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

In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by adding length validation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9350.

CVE-2017-11411 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=a83a324acdfc07a0ca8b65e6ebaba3374ab19c76
Wireshark - wwna-sec-2017-28	Vendor Advisory	CONFIRM www.wireshark.org/security/wnna-sec-2017-28.html

Wireshark - WMPA SEC 2017-20
openSAFETY dissector memory
exhaustion

Vendor Advisory

www.wireshark.org

text/html

[CONFIRM http://www.wireshark.org/security/wmpa-sec-2017-20.html](http://www.wireshark.org/security/wmpa-sec-2017-20.html)

13755 – [oss-fuzz] Allocation too
large: 4294967295 > 2147483648
(0xffffffff > 0x80000000)

Issue Tracking

Patch

Vendor Advisory

bugs.wireshark.org

text/html

 [CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=13755](https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13755)

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	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	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	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All
Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All

Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	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	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All
Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	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:2.0.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.11:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.12:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.13:*:*:*:*:*:						
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:2.0.5:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.6:*:*:*:*:*:						

```
cpe:2.3:a:wireshark:wireshark:2.0.7:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.8:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wreshark:wreshark:2.2.0:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.2.1:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:2.2.2:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.5:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.2.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.1:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.10:*.:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.11:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.12:*:*:*:*:*:*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.13:*:*:*:*:*:
```

```
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:2.0.5:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.8:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.0.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.0:*.~*~*~*~*~*
```

```
cpe:2.3:a:wireshark:wireshark:2.2.1:::~::~:
```

```
cpe:2.3:a:wireshark:wireshark:2.2.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:wireshark:wireshark:2.2.3:*:*:*:*:*.*
```

cpe:2.3:a:wireshark:wireshark:2.2.4:*****:
cpe:2.3:a:wireshark:wireshark:2.2.5:*****:
cpe:2.3:a:wireshark:wireshark:2.2.6:*****:
cpe:2.3:a:wireshark:wireshark:2.2.7:*****:

No vendor comments have been submitted for this CVE

← Previous IDNext ID →

© [CVE.report](#) 2023  |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)