

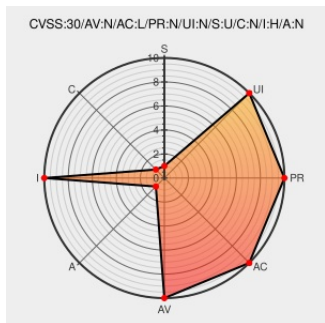


# CVE-2017-8855

Published on: 05/09/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

## CVE-2017-8855

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

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

wolfSSL before 3.11.0 does not prevent wc\_DhAgree from accepting a malformed DH key.

CVE-2017-8855 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                               | Tags                                                                                                                                                       | Link                                                                                                                                                           |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Release wolfSSL version 3.11.0 · wolfSSL/wolfssl · GitHub | <a href="#">Issue Tracking</a><br><a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM</a><br><a href="https://github.com/wolfSSL/wolfssl/releases/tag/v3.11.0-stable">github.com/wolfSSL/wolfssl/releases/tag/v3.11.0-stable</a> |

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](mailto: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                      | <a href="#">Wolfssl</a> | <a href="#">Wolfssl</a> | All     | All    | All     | All      |
| cpe:2.3:a:wolfssl:wolfssl:*****: |                         |                         |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)