



CVE-2017-2800

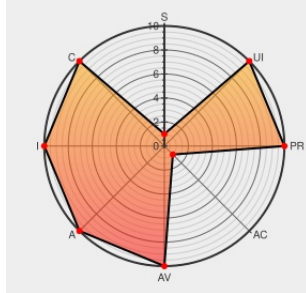
Published on: 05/24/2017 12:00:00 AM UTC

Last Modified on: 01/28/2023 02:01:00 AM UTC

CVE-2017-2800

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

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



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

A specially crafted x509 certificate can cause a single out of bounds byte overwrite in wolfSSL through 3.10.2 resulting in potential certificate validation vulnerabilities, denial of service and possible remote code execution. In order to trigger this vulnerability, the attacker needs to supply a malicious x509 certificate to either a server or a client application using this library.

CVE-2017-2800 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [cisco](#) **wolfSSL** - **wolfSSL** version **3.10.2**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

wolfSSL 3.10.2 - x509 Certificate Text Parsing Off-by-One - Multiple dos Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

EXPLOIT-DB 41984

TALOS-2017-0293 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

[Exploit](#)
[Third Party Advisory](#)
[talosintelligence.com](#)
[text/html](#)

MISC
[talosintelligence.com/vulnerability_reports/TALOS-2017-0293](#)

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	Wolfssl	Wolfssl	All	All	All	All

cpe:2.3:a:wolfssl:wolfssl:*****:*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)