



CVE-2018-1000159

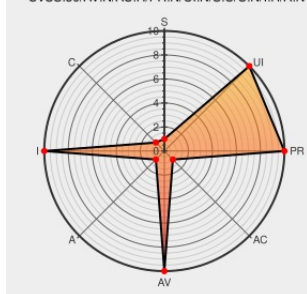
Published on: 04/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000159

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

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



Certain versions of [Tlsite-ng](#) from [Tlsite-ng Project](#) contain the following vulnerability:

tlsite-ng version 0.7.3 and earlier, since commit d7b288316bca7bcdd082e6ccff5491e241305233 contains a CWE-354: Improper Validation of Integrity Check Value vulnerability in TLS implementation, `tlsite/utls/constanttime.py`:

`ct_check_cbc_mac_and_pad()`; line "end_pos = data_len - 1 -

mac.digest_size" that can result in an attacker manipulating the TLS ciphertext which will not be detected by receiving tlsite-ng. This attack appears to be exploitable via man in the middle on a network connection. This vulnerability appears to have been fixed after commit 3674815d1b0f7484454995e2737a352e0a6a93d8.

CVE-2018-1000159 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description

verify the mac even if the padding is 1 byte long by tomato42 · Pull Request #234 · tlsfuzzer/tlslite-ng · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

MISC

github.com/tomato42/tlslite-ng/pull/234

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.

Related QID Numbers

981118 Python (pip) Security Update for tlslite-ng (GHSA-cwh5-3cw7-4286)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tlslite-ng Project	Tlslite-ng	All	All	All	All
cpe:2.3:a:tlslite-ng_project:tlslite-ng:*****::						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→