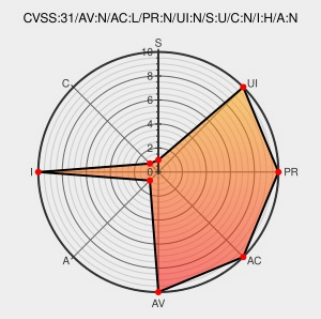
CVE-2020-26263

Published on: 12/21/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26263 - advisory for GHSA-wvcv-832q-fjg7

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tlslite-ng from Tlslite-ng Project contain the following vulnerability:

tlslite-ng is an open source python library that implements SSL and TLS cryptographic protocols. In tlslite-ng before versions 0.7.6 and 0.8.0-alpha39, the code that performs decryption and padding check in RSA PKCS#1 v1.5 decryption is data dependant. In particular, the code has multiple ways in which it leaks information about the decrypted ciphertext. It aborts as soon as the plaintext doesn't start with 0x00, 0x02. All TLS servers that enable RSA key exchange as well as applications that use the RSA decryption API directly are vulnerable. This is patched in versions 0.7.6 and 0.8.0-alpha39. Note: the patches depend on Python processing the individual bytes in side-channel free manner, this is known to not the case (see reference). As such, users that require side-channel resistance are recommended to use different TLS implementations, as stated in the security policy of tlslite-ng.

CVE-2020-26263 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tlsfuzzer** - **tlslite-ng** version **< 0.7.6**

Affected Vendor/Software: **tlsfuzzer** - **tlslite-ng** version **>= 0.8.0-alpha1, < 0.8.0-alpha39**

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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
tlslite-ng · PyPI	Product, Third Party Advisory, pypi.org, text/html	MISC pypi.org/project/tlslite-ng/
Bleichenbacher fixes [0.7] by tomato42 · Pull Request #439 · tlsfuzzer/tlslite-ng · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tlsfuzzer/tlslite-ng/pull/439
Attempt side-channel free RSA decryption by tomato42 · Pull Request #438 · tlsfuzzer/tlslite-ng · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tlsfuzzer/tlslite-ng/pull/438
“Constant time” compare in Python | securitypitfalls	Exploit, Third Party Advisory, securitypitfalls.wordpress.com, text/html	MISC securitypitfalls.wordpress.com/2018/08/03/constant-time-compare-in-python/
Merge pull request #439 from tlsfuzzer/bleichenbacher-fixes-0.7 · tlsfuzzer/tlslite-ng@c28d6d3 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tlsfuzzer/tlslite-ng/commit/c28d6d387bba59d8bd5cb3ba15edc42edf54b368
Bleichenbacher timing side-channel oracle in PKCS#1 v1.5 decryption · Advisory · tlsfuzzer/tlslite-ng · GitHub	Exploit, Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/tlsfuzzer/tlslite-ng/security/advisories/GHSA-wvcv-832q-fjg7

Related QID Numbers

983233 Python (pip) Security Update for tlslite-ng (GHSA-wvcv-832q-fjg7)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tlslite-ng Project	Tlslite-ng	All	All	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha1	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha10	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha11	All	All

Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha12	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha13	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha14	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha15	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha16	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha17	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha18	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha19	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha2	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha20	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha21	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha22	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha23	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha24	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha25	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha26	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha27	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha28	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha29	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha3	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha30	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha31	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha32	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha33	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha34	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha35	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha36	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha37	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha38	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha4	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha5	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha6	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha7	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha8	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha9	All	All
Application	Tlslite-ng Project	Tlslite-ng	All	All	All	All

Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha1	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha10	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha11	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha12	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha13	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha14	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha15	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha16	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha17	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha18	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha19	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha2	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha20	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha21	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha22	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha23	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha24	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha25	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha26	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha27	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha28	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha29	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha3	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha30	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha31	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha32	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha33	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha34	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha35	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha36	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha37	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha38	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha4	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha5	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha6	All	All

Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha7	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha8	All	All
Application	Tlslite-ng Project	Tlslite-ng	0.8.0	alpha9	All	All

- cpe:2.3:a:tlslite-ng_project:tlslite-ng:*:*:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha1:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha10:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha11:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha12:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha13:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha14:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha15:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha16:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha17:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha18:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha19:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha2:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha20:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha21:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha22:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha23:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha24:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha25:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha26:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha27:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha28:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha29:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha3:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha30:*:*:*:*:*:*:
- cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha31:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha32:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha33:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha34:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha35:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha36:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha37:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha38:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha4:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha5:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha6:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha7:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha8:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha9:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:*:*:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha1:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha10:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha11:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha12:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha13:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha14:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha15:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha16:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha17:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha18:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha19:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha2:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha20:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha21:*:*:*:*:*:*:*

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha22:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha23:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha24:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha25:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha26:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha27:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha28:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha29:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha3:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha30:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha31:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha32:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha33:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha34:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha35:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha36:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha37:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha38:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha4:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha5:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha6:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha7:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha8:*:*:*:*:*:*:

cpe:2.3:a:tlslite-ng_project:tlslite-ng:0.8.0:alpha9:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report