



CVE-2020-20949

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-20949
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-20 16:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	Bleichenbacher's attack on PKCS #1 v1.5 padding for RSA in STM32 cryptographic firmware library software expansion for

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	letf	Public Key Cryptography Standards 1	1.5	All	All	All
Application	letf	Public Key Cryptography Standards 1	1.5	All	All	All
Application	St	Stm32cubef0	-	All	All	All
Application	St	Stm32cubef0	-	All	All	All
Application	St	Stm32cubef1	-	All	All	All
Application	St	Stm32cubef1	-	All	All	All
Application	St	Stm32cubef2	-	All	All	All
Application	St	Stm32cubef2	-	All	All	All
Application	St	Stm32cubef3	-	All	All	All
Application	St	Stm32cubef3	-	All	All	All
Application	St	Stm32cubef4	-	All	All	All
Application	St	Stm32cubef4	-	All	All	All
Application	St	Stm32cubef7	-	All	All	All
Application	St	Stm32cubef7	-	All	All	All
Application	St	Stm32cubeg0	-	All	All	All
Application	St	Stm32cubeg0	-	All	All	All
Application	St	Stm32cubeg4	-	All	All	All

Application	St	Stm32cubeg4	-	All	All	All
Application	St	Stm32cubeh7	-	All	All	All
Application	St	Stm32cubeh7	-	All	All	All
Application	St	Stm32cubeide	-	All	All	All
Application	St	Stm32cubeide	-	All	All	All
Application	St	Stm32cubel0	-	All	All	All
Application	St	Stm32cubel0	-	All	All	All
Application	St	Stm32cubel1	-	All	All	All
Application	St	Stm32cubel1	-	All	All	All
Application	St	Stm32cubel4	-	All	All	All
Application	St	Stm32cubel4	-	All	All	All
Application	St	Stm32cubel4	-	All	All	All
Application	St	Stm32cubel4	-	All	All	All
Application	St	Stm32cubel4	-	All	All	All
Application	St	Stm32cubel5	-	All	All	All
Application	St	Stm32cubel5	-	All	All	All
Application	St	Stm32cubemonitor	-	All	All	All
Application	St	Stm32cubemonitor	-	All	All	All
Application	St	Stm32cubemp1	-	All	All	All
Application	St	Stm32cubemp1	-	All	All	All
Application	St	Stm32cubemx	-	All	All	All
Application	St	Stm32cubemx	-	All	All	All
Application	St	Stm32cubeprogrammer	-	All	All	All
Application	St	Stm32cubeprogrammer	-	All	All	All
Application	St	Stm32cubewb	-	All	All	All
Application	St	Stm32cubewb	-	All	All	All
Application	St	Stm32cubewl	-	All	All	All
Application	St	Stm32cubewl	-	All	All	All

References

Reference

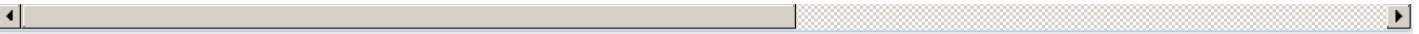
Silence Will Fall (Or How It Can Take 2 Years to Get Your Vuln Registered) | by BI.ZONE | Jan, 2021 | Medium

archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf

ST

X-CUBE-CRYPTOLIB - STM32 cryptographic firmware library software expansion for STM32Cube (UM1924) - STMicroelectronics - STMicroelectronics

[x-cube-cryptolib.com](https://www.st.com/en/development-tools/x-cube-cryptolib.html)



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)