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	Ietf	Public Key Cryptography Standards 1	1.5	All	All	All
Application	Ietf	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	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 - STMicroe
x-cube-cryptolib.com

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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