CVE-2019-16863

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-16863
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-14 03:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	STMicroelectronics ST33TPHF2ESPI TPM devices before 2019-09-12 allow attackers to extract the ECDSA private key via

Risk And Classification

Problem Types: CWE-327 | CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	St	St33tphf20i2c	-	All	All	All
Operating System	St	St33tphf20i2c Firmware	74.5	All	All	All
Operating System	St	St33tphf20i2c Firmware	74.9	All	All	All
Hardware	St	St33tphf20spi	-	All	All	All
Operating System	St	St33tphf20spi Firmware	74.0	All	All	All
Operating System	St	St33tphf20spi Firmware	74.16	All	All	All
Operating System	St	St33tphf20spi Firmware	74.4	All	All	All
Operating System	St	St33tphf20spi Firmware	74.8	All	All	All
Hardware	St	St33tphf2ei2c	-	All	All	All
Operating System	St	St33tphf2ei2c Firmware	73.5	All	All	All
Operating System	St	St33tphf2ei2c Firmware	73.9	All	All	All
Hardware	St	St33tphf2espi	-	All	All	All
Hardware	St	St33tphf2espi	-	All	All	All
Hardware	St	St33tphf2espiqfn	-	All	All	All
Hardware	St	St33tphf2espiqfn	-	All	All	All
Operating System	St	St33tphf2espiqfn Firmware	All	All	All	All
Operating System	St	St33tphf2espiqfn Firmware	All	All	All	All

Hardware	St	St33tphf2espir28	-	All	All	All
Hardware	St	St33tphf2espir28	-	All	All	All
Operating System	St	St33tphf2espir28 Firmware	All	All	All	All
Operating System	St	St33tphf2espir28 Firmware	All	All	All	All
Operating System	St	St33tphf2espi Firmware	All	All	All	All
Operating System	St	St33tphf2espi Firmware	71.0	All	All	All
Operating System	St	St33tphf2espi Firmware	71.12	All	All	All
Operating System	St	St33tphf2espi Firmware	71.4	All	All	All
Operating System	St	St33tphf2espi Firmware	73.0	All	All	All
Operating System	St	St33tphf2espi Firmware	73.4	All	All	All
Operating System	St	St33tphf2espi Firmware	73.8	All	All	All
Operating System	St	St33tphf2espi Firmware	All	All	All	All

References

Reference	Source	Link
myF5		support.f5.com
ST Microelectronics TPM Firmware ECDSA Signature Generation Vulnerability - US	CONFIRM	support.lenovo.com
support.f5.com/csp/article/K32412503	CONFIRM	support.f5.com
TPM-FAIL Attack	MISC	tpm.fail
Document Display | HPE Support Center	CONFIRM	support.hpe.com
TPM update - STMicroelectronics	CONFIRM	www.st.com
portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190024	MISC	portal.msrc.microsoft
CONFIRM:https://support.f5.com/csp/article/K32412503?utm_source=f5support&utm_medium=RSS	MITRE	support.f5.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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