CVE-2020-20950

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-20950
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-19 13:15:00 UTC
Updated	2021-09-08 17:22:00 UTC
Description	Bleichenbacher's attack on PKCS #1 v1.5 padding for RSA in Microchip Libraries for Applications 2018-11-26 All up to 2018

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Application	Ietf	Public Key Cryptography Standards 1	1.5	All	All	All
Application	Ietf	Public Key Cryptography Standards 1	1.5	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Microchip	Microchip Libraries For Applications	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link
Silence Will Fall (Or How It Can Take 2 Years to Get Your Vuln Registered) | by BI.ZONE | Jan, 2021 | Medium	MISC	bi-zone.mediu
microchip.com	MISC	microchip.com
archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf	MISC	archiv.infsec.e
Microchip Libraries for Applications | Microchip Technology Inc.	MISC	www.microchi

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.