



# CVE-2020-20950

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

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

## Risk And Classification

**Problem Types:** CWE-327

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os</a>	-	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os</a>	-	All	All	All
Application	<a href="#">letf</a>	<a href="#">Public Key Cryptography Standards 1</a>	1.5	All	All	All
Application	<a href="#">letf</a>	<a href="#">Public Key Cryptography Standards 1</a>	1.5	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Application	<a href="#">Microchip</a>	<a href="#">Microchip Libraries For Applications</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	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	<a href="#">bi-zone.medium.com</a>
microchip.com	MISC	<a href="#">microchip.com</a>
archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf	MISC	<a href="#">archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf</a>
Microchip Libraries for Applications   Microchip Technology Inc.	MISC	<a href="#">www.microchip.com</a>

CVE Program record

CVE.ORG [www.cve.org](http://www.cve.org)

NVD vulnerability detail

NVD [nvd.nist.gov](http://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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)