



CVE-2020-25657

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2020-25657
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-12 15:15:00 UTC
Updated	2023-02-12 23:40:00 UTC
Description	A flaw was found in all released versions of m2crypto, where they are vulnerable to Bleichenbacher timing attacks in the RS

Risk And Classification

Problem Types: CWE-385

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	M2crypto Project	M2crypto	All	All	All	All
Application	M2crypto Project	M2crypto	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.re
1889823 – (CVE-2020-25657) CVE-2020-25657 m2crypto: bleichenbacher timing attacks in the RSA decryption API	MISC	bugzilla.re
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.re
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[752378](#) SUSE Enterprise Linux Security Update for python-M2Crypto (SUSE-SU-2022:2532-1)

[752383](#) SUSE Enterprise Linux Security Update for python-M2Crypto (SUSE-SU-2022:2527-1)

[752396](#) SUSE Enterprise Linux Security Update for python-M2Crypto (SUSE-SU-2022:2562-1)

[752448](#) SUSE Enterprise Linux Security Update for python-M2Crypto (SUSE-SU-2022:2691-1)

[900223](#) CBL-Mariner Linux Security Update for m2crypto 0.35.2

[900984](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (6675)

[902449](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10079)

[902454](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10076)

[902461](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10125)

[902468](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10108)

[902513](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10079)

[902520](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10076)

[903842](#) Common Base Linux Mariner (CBL-Mariner) Security Update for m2crypto (10076-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)