



CVE-2021-3798

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

Summary

CVE	CVE-2021-3798
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 16:15:00 UTC
Updated	2023-07-10 19:34:00 UTC
Description	A flaw was found in openCryptoki. The openCryptoki Soft token does not check if an EC key is valid when an EC key is cre

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencryptoki Project	Opencryptoki	All	All	All	All

References

Reference	Source
SOFT: Check the EC Key on C_CreateObject and C_DeriveKey by ifranzki · Pull Request #402 · opencryptoki/opencryptoki · GitHub	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
SOFT: Check the EC Key on C_CreateObject and C_DeriveKey · opencryptoki/opencryptoki@4e3b43c · GitHub	MISC
1990591 – (CVE-2021-3798) CVE-2021-3798 openCryptoki: Soft token does not check if an EC key is valid	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[903805](#) Common Base Linux Mariner (CBL-Mariner) Security Update for opencryptoki (10659)

[907285](#) Common Base Linux Mariner (CBL-Mariner) Security Update for opencryptoki (10659-1)

© [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](#)