CVE-2021-3798

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

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 crea

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	Sourc
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)