



CVE-2012-4455

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

Summary

CVE	CVE-2012-4455
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-10 18:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	openCryptoki 2.4.1 allows local users to create or set world-writable permissions on arbitrary files via a symlink attack on th

Risk And Classification

Primary CVSS: v2.0 6.2 from nvd@nist.gov

AV:L/AC:H/Au:N/C:C/I:C/A:C

Problem Types: CWE-59 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:H/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencryptoki Project	Opencryptoki	2.4.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

openCryptoki / [Opencryptoki-tech] opencryptoki release 2.4.2

oss-security - Re: CVE request: opencryptoki insecure lock files handling

IBM X-Force Exchange

openCryptoki Multiple Insecure File Creation Vulnerabilities

730636 – (CVE-2012-4454, CVE-2012-4455) CVE-2012-4454 CVE-2012-4455 opencryptoki: insecure handling of files in the /tmp directory

openCryptoki / None tools

oss-security - Re: CVE request: opencryptoki insecure lock files handling

oss-security - Re: CVE request: opencryptoki insecure lock files handling

oss-security - Re: CVE request: opencryptoki insecure lock files handling

oss-security - Re: CVE request: opencryptoki insecure lock files handling

Security Alerts - Secunia

oss-security - CVE request: opencryptoki insecure lock files handling

openCryptoki / None tools

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)