



CVE-2002-1446

Published on: 08/01/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

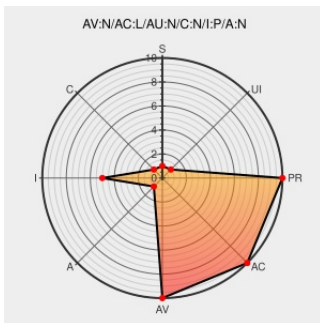
CVE-2002-1446

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Pkcs 11 Library](#) from [Ncipher](#) contain the following vulnerability:

The error checking routine used for the C_Verify call on a symmetric verification key in the nCipher PKCS#11 library 1.2.0 and later returns the CKR_OK status even when it detects an invalid signature, which could allow remote attackers to modify or forge messages.

CVE-2002-1446 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Neohapsis Archives - Bugtraq - nCipher Advisory #5: C_Verify validates incorrect symmetric signatures - From technotifications_at_us.ncipher.com

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[BUGTRAQ 20020819 nCipher Advisory #5: C_Verify validates incorrect symmetric signatures](#)

C_Verify validates incorrect symmetric signatures

[Patch](#)

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[CONFIRM](#)
[www.ncipher.com/support/advisories/advisory5_c_verify.html](#)

ISS X-Force Database: ncipher-cverify-improper-verification (9895): nCipher PKCS#11 library C_Verify performs improper validation of symmetric signatures

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[XF ncipher-cverify-improper-verification\(9895\)](#)

nCipher PKCS#11 Symmetric Message Signature Verification Vulnerability

[cve.report \(archive\)](#)

[text/html](#)

[BID 5498](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ncipher	Pkcs 11 Library	1.2.0	All	All	All
Application	Ncipher	Pkcs 11 Library	1.2.0	All	All	All
cpe:2.3:a:ncipher:pkcs_11_library:1.2.0:*****:*						
cpe:2.3:a:ncipher:pkcs_11_library:1.2.0:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)