



CVE-2006-1117

Published on: 03/09/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

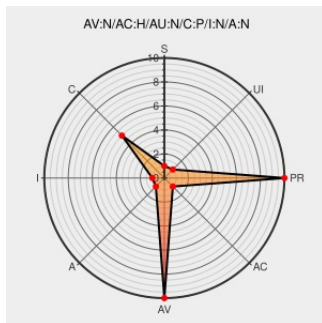
CVE-2006-1117

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Dse200 Document Sealing Engine](#) from [Ncipher](#) contain the following vulnerability:

nCipher firmware before V10, as used by (1) nShield, (2) nForce, (3) netHSM, (4) payShield, (5) SecureDB, (6) DSE200 Document Sealing Engine, (7) Time Source Master Clock (TSMC), and possibly other products, contains certain options that were only intended for testing and not production, which might allow remote attackers to obtain information about encryption keys and crack those keys with less effort than brute force.

CVE-2006-1117 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
nCipher - SA#14: Presence of flaws in firmware security	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.ncipher.com/resources/97/sa14_presence_of_flaws_in_firmware_security
Secunia - Advisories - nCipher Products Multiple Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19137
Webmail : Solution de messagerie professionnelle OVHcloud OVH	www.vupen.com text/html	VUPEN ADV-2006-0862

nCipher Testing Options Insecure Key Generation Vulnerabilities	Patch cve.report (archive) text/html	 BID 17012
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20060309 nCipher Advisory #14: Presence of flaws in firmware security
SecurityTracker.com Archives - nCipher nCore May Let Users Conduct Key Determination Attacks and May Fail to Detect MAC Message Modification	Patch Vendor Advisory securitytracker.com text/html	 SECTrack 1015718
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ncipher-firmware-weak-security(25063)

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	Dse200 Document Sealing Engine	All	All	All	All
Application	Ncipher	Dse200 Document Sealing Engine	All	All	All	All
Application	Ncipher	Ncore	All	All	All	All
Application	Ncipher	Ncore	All	All	All	All
Hardware  	Ncipher	Nethsm	2.0	All	All	All
Hardware  	Ncipher	Nethsm	2.1	All	All	All
Hardware  	Ncipher	Nethsm	2.1.12_cam5	All	All	All
Hardware  	Ncipher	Nethsm	2.0	All	All	All
Hardware  	Ncipher	Nethsm	2.1	All	All	All
Hardware  	Ncipher	Nethsm	2.1.12_cam5	All	All	All
Application	Ncipher	Nforce	All	All	All	All
Application	Ncipher	Nforce	All	All	All	All
Hardware  	Ncipher	Nshield	All	All	All	All
Hardware  	Ncipher	Nshield	All	All	All	All
Hardware  	Ncipher	Payshield	All	All	All	All
Hardware  	Ncipher	Payshield	All	All	All	All

Application	Ncipher	Securedb	All	All	All	All
Application	Ncipher	Securedb	All	All	All	All
Application	Ncipher	Time Source Master Clock	All	All	All	All
Application	Ncipher	Time Source Master Clock	All	All	All	All
cpe:2.3:a:ncipher:dse200_document_sealing_engine:*****:						
cpe:2.3:a:ncipher:dse200_document_sealing_engine:*****:						
cpe:2.3:a:ncipher:ncore:*****:						
cpe:2.3:a:ncipher:ncore:*****:						
cpe:2.3:h:ncipher:nethsm:2.0:*****:						
cpe:2.3:h:ncipher:nethsm:2.1:*****:						
cpe:2.3:h:ncipher:nethsm:2.1.12_cam5:*****:						
cpe:2.3:h:ncipher:nethsm:2.0:*****:						
cpe:2.3:h:ncipher:nethsm:2.1:*****:						
cpe:2.3:h:ncipher:nethsm:2.1.12_cam5:*****:						
cpe:2.3:a:ncipher:nforce:*****:						
cpe:2.3:a:ncipher:nforce:*****:						
cpe:2.3:h:ncipher:nshield:*****:						
cpe:2.3:h:ncipher:nshield:*****:						
cpe:2.3:h:ncipher:payshield:*****:						
cpe:2.3:h:ncipher:payshield:*****:						
cpe:2.3:a:ncipher:securedb:*****:						
cpe:2.3:a:ncipher:securedb:*****:						
cpe:2.3:a:ncipher:time_source_master_clock:*****:						
cpe:2.3:a:ncipher:time_source_master_clock:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

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