

# [NEWS] MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0063.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/13/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Mon, 13 May 2002 21:01:25 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat

---

## SUMMARY

In certain circumstances, the nCipher MSCAPI CSP Install Wizard support software on Windows 2000 will set the nCipher CSP key generation behavior incorrectly. Despite the user requesting Operator Card Set protection for keys ('cardset protected keys') that are generated using the nCipher CSP, a software error might result in keys being protected by the module alone.

## DETAILS

Vulnerable systems:

nCipher CSP version 5.50

Immune systems:

nCipher CSP versions above 5.50

Background:

1. Security world

nCipher's key management modules (nForce / nShield) are generally used with nCipher's suite of utilities for managing a 'security world'. A security world is a collection of cryptographic keys, smart cards, modules, and associated data stored on host computers. A security world is

## Securiteam: [NEWS] MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat

designed to prevent unauthorized access to application keys while maintaining scalability and key availability.

The core security world secrets are protected by Administrator Cards written by the initialization software and kept safe by the user.

Either application keys can be made available to any nCipher module appropriately programmed with the user's Administrator Cards (module-protected keys) or they can be protected by further smart cards known as Operator Cards that provide an additional layer of security.

### 2. The nCipher CSP

If the CSP is set up to use module-protected keys, when applications tell the CSP to create a key, it needs no input from the user. If the CSP is set up to use Operator Cards and is told to create a key, it first looks to see if there are any cards which it can load automatically, and uses those if any are present. If not, it prompts the user to choose which Operator Card Set to use.

Issue description:

#### 1. Cause

The Install Wizard for the nCipher CSP support software on Windows 2000 offers a check box for controlling whether a key to be generated is module protected or to be additionally protected by an Operator Card Set.

When the Install Wizard is used to create an Operator Card Set then the nCipher CSP key generation behaves as requested by the user.

If cardset protection is selected from the Install Wizard but a new Operator Card Set is \*not\* created, the wizard incorrectly sets the nCipher CSPs up to use module protection for all keys that they subsequently create.

#### 2. Impact

If the user is affected by this issue, any application key generated by the nCipher CSP will be incorrectly protected by the module alone, rather than by a combination of operator card set and module.

This means that an attacker, who gains control of any nCipher module that has been programmed into the key's security world can gain unauthorized access to this key, since no further smart card authorization is required.

#### 3. Who May Be Affected

This problem only affects keys that have been generated by the nCipher CSP after the Install Wizard from CD version 5.50 has been run.

The problem does not affect keys that were:

- \* Generated by any software other than the nCipher CSP, or
- \* Generated by the nCipher CSP using the Install Wizard from any CD other than version 5.50.

## Securiteam: [NEWS] MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat

### 4. How to Tell If You Are Affected

To find out whether you're affected, run ``c:\nfast\bin\csputils.exe -d`` from the command line. This will give you a detailed summary of all your containers and information for the keys they contain.

Each key (key exchange and/or signature) will have a description including whether or not it was generated by the nCipher CSP, its hash, and its protection method.

A cardset-protected key (here stored in a container called ``expimptst``) will have an entry like the following (lines have been truncated for clarity):

Detailed report for container ID `#cbfb7b11909b40ddc50da759d6029...`

Filename: `key_mscapi_container-cbfb7b11909b40ddc50da759d6...`

Container name: `expimptst`

User name: `NCIPHER\james`

User SID: `s-1-5-21-1594850079-719136693-34565100-1111`

CSP DLL name: `ncsp.dll`

No signature key.

Filename for key exchange key is `key_mscapi_expimptst-ncsp-ujam...`

Key was generated by the CSP

Key hash: `92c60edf376c26e9ee76db3a2a70dd031636a218`

Key is recoverable.

Key is cardset protected.

Cardset name: `mscapi-grimsby`

Sharing parameters: 1 of 1 shares required.

Cardset hash: `4eb80f966c13bd735cb50f29ef19e5e...`

Cardset is persistent.

And a module protected key will have one like the following:

Filename: `key_mscapi_container-32a16394a3ffe52eb4db1127d8...`

Container name: `james`

User name: `NCIPHER\james`

User SID: `s-1-5-21-1594850079-719136693-34565100-1111`

CSP DLL name: `ncsp.dll`

No signature key.

Filename for key exchange key is `key_mscapi_6fa4c59efefb6c01db6...`

Key was generated by the CSP

Key hash: `6fa4c59efefb6c01db6eca9f1eadbb17158fc2a8`

Key is recoverable.

Key is module protected.

If you have keys unexpectedly module protected when they should be cardset protected you are affected by this bug.

Remedy:

1. Users who have NOT already created a key with the wrong protection  
In order to force MSCAPI applications to generate cardset-protected keys a

Securiteam: [NEWS] MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat

file `wizardfix.reg' should be created containing the following text:

```
----- CUT HERE -----
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\nCipher\Cryptography]
"UseModuleKeys"=dword:00000000
----- CUT HERE -----
```

This file can then be run by the user to change the appropriate registry entry that determines the behavior of key generation using the nCipher CSP.

Alternatively, the user can edit the registry value specified above directly using `regedit'.

The registry setting must be reset using either of the above methods after each invocation of the affected nCipher CSP Install Wizard.

2. Users who have already created a key that is erroneously module protected  
 Users, who have already generated keys that were intended to be cardset protected, but due to this error are not, are advised to apply the above registry fix and generate new keys. nCipher recommends against converting existing module-protected keys to cardset-protected status, since it is extremely difficult to do this in a way that increases security.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[support@nCIPHER.com](mailto:support@nCIPHER.com)> nCipher Support.

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
 To unsubscribe from the list, send mail with an empty subject line and body to:  
[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)  
 In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.  
 In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] Cibleclick.com Stores Passwords in Clear Text inside Cookies"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)