

[NEWS] payShield Library Bad Requests Verification

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/15/04

To: list@securiteam.com

Date: 15 Jan 2004 17:58:45 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

payShield Library Bad Requests Verification

SUMMARY

When a command is issued to the payShield SPP library it may return Status_OK regardless of what the real reply status was.

DETAILS

When a command is sent through the SPP library the library may query its HSMs to ensure they are responsive and working properly. When this check is triggered and successful, the response to the original command will always be Status_OK, regardless of what status code the HSM returned.

Although an error message will be printed to the payShield log this error is not communicated to the calling function.

During constant use, this event will occur once every three minutes, regardless of the number of threads or HSMs employed.

Impact:

The issue is in the host-side library and applications only. Existing payShield installations and keys are not compromised and may continue to

Securiteam: [NEWS] payShield Library Bad Requests Verification

be used with the new software.

The issue does not reveal any information about secret keys or data, it only leads to a risk of false-positive verifications.

If the command being processed when the modules query is triggered is supposed to return a non-0 status code, this status will be lost.

For example, an invalid PIN verification attempt will result in Status_VerifyFailed being returned from the HSM, but the library call SPP_VerifyPVV() may return Status_OK, making it appear that the PIN was valid. If an attacker had sole access to the payShield application and were able to flood it with invalid requests then they would eventually get an 'OK' response.

One way to detect this would be retrospective review of payShield error logs.

Who Is *Not* Affected:

Customers not using payShield are unaffected.

Customers not using versions 1.3.12, 1.5.18, and 1.6.18 of the SPP library are unaffected.

Also, customers who use payShield solely for 'none' and 'HMAC' key establishment (ie those not using the SPP library for payments processing) are not affected. However, we still suggest that these customers update their software in order to avoid potential future use of affected software.

Who Is Affected:

Application developers linking against versions 1.3.12, 1.5.18 and 1.6.18 of the SPP library and their end-users will be affected. If your version number is between 1.3.12 and 1.6.18 but does not appear in the list, please contact nCipher support and quote your version number.

How To Tell If You Are Affected:

Run the nversions utility on the development machine and look for "emvspp devel". If this includes "1.3.12", "1.5.18" or "1.6.18" then you are affected. If you do not have nversions then look in the file \$NFAST_HOME/lib/versions/emvspp-devel-atv.txt for this information.

This version number can also be queried by calling the library functions SPP_GetLibVersion() or SPP_PrintLibVersion().

Alternatively flood your application with bad verification requests (for example modify the value of the pvv key vector in knownvectors.h, rebuild the sppbenchmark example and run the pvv benchmark test) and watch for Status_OK. If you are affected then 1 command in any 3 minute window will return Status_OK. All others will return the appropriate error code.

Securiteam: [NEWS] payShield Library Bad Requests Verification

Remedy:

Detection:

In existing applications linked against affected versions of the library any erroneous 'OK' response can be detected through log auditing, this is not a means of prevention. A normal failure report will print 2 consecutive messages:

```
<time> [Error] In <function>, SEEJob reply status not OK  
      (status VerifyFailed)
```

```
<time> [Error] In SPP_<function>, Sending SEEJob failed  
      (status VerifyFailed)
```

But an affected application will only report:

```
<time> [Error] In <function>, SEEJob reply status not OK  
      (status VerifyFailed)
```

Higher levels of reporting will also print 'OK' [Info] messages after the [Error].

Work-around:

There is a work-around to this problem, but it is more intrusive than relinking with the new library. Since the issue only affects one call in any three-minute period the work-around is to make each call into the SPP library twice and check both error codes.

Recommended course of action:

Developer customers should update their software and re-link their applications with the fixed library at the earliest opportunity. This is more effective and less intrusive than the work-around.

End users should contact their application vendor for an updated application.

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:technotifications@us.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

In order to subscribe to the mailing list, simply forward this email to: 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,

Securiteam: [NEWS] payShield Library Bad Requests Verification

loss of business profits or special damages.