

TYPO3.Flow - Bug # 36767

Status:	Resolved	Priority:	Must have
Author:	Alexander Berl	Category:	Security
Created:	2012-05-02	Assigned To:	
Updated:	2012-05-22	Due date:	
PHP Version:	5.3		
Has patch:	Yes		
Complexity:	no-brainer		
Affected Flow version:	Git master		
Subject:	generateHmac does not use safe getEncryptionKey leading to possibly invalid hmacs		
Description	<p>Currently the generateHmac function of the Security\Cryptography\HashService directly accesses <i>\$this->encryptionKey</i> instead of using the (lazy loading) getter.</p> <p>Hence under certain circumstances the encryptionKey may still be unloaded leading to wrong hmacs being generated, only being noticed when the hmac validation fails later on.</p>		

Associated revisions

Revision 66312551 - 2012-05-21 14:18 - Ferdinand Kuhl

[BUGFIX] generateHmac method does not use safe getEncryptionKey

The generateHmac function uses encryptionKey property directly and not through the safe getEncryptionKey method, leading to uninitialized access without having an encryptionKey set.

Change-Id: I35665ee459f1c5cd9afee70db38fe7a1da7cb86d

Fixes: #36767

Releases: 1.1, 1.2

Revision 7c1cadb7 - 2012-05-21 14:21 - Ferdinand Kuhl

[BUGFIX] generateHmac method does not use safe getEncryptionKey

The generateHmac function uses encryptionKey property directly and not through the safe getEncryptionKey method, leading to uninitialized access without having an encryptionKey set.

Change-Id: I26d58cc91d7c934295995f81b7a436ffce2dee92

Fixes: #36767

Releases: 1.1, 1.2

History

#1 - 2012-05-17 15:17 - Gerrit Code Review

- Status changed from New to Under Review

Patch set 1 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/11273>

#2 - 2012-05-18 10:00 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/11273>

#3 - 2012-05-21 14:20 - Gerrit Code Review

Patch set 3 for branch **master** has been pushed to the review server.

It is available at <http://review.typo3.org/11273>

#4 - 2012-05-21 14:21 - Gerrit Code Review

Patch set 1 for branch **FLOW3-1.1** has been pushed to the review server.

It is available at <http://review.typo3.org/11366>

#5 - 2012-05-22 02:41 - Ferdinand Kuhl

- *Status changed from Under Review to Resolved*

- *% Done changed from 0 to 100*

Applied in changeset commit:7c1cabb78710f05da01c9208ad39470edb8df310.

Files

0001-BUG-Fix-hash-service-hmac-generation-is-wrong-when-n.patc	985 Bytes	2012-05-02	Alexander Berl
----------------------------------------------------------------	-----------	------------	----------------