TYPO3.Flow - Bug # 35300

Status:	Resolved	**Priority:**	Must have
Author:	Andreas Förthner	**Category:**	Security
Created:	2012-03-28	**Assigned To:**	Andreas Förthner
Updated:	2012-04-15	**Due date:**	2012-03-28
PHP Version:	5.3		
Has patch:	Yes		
Complexity:	easy		
Affected Flow version:	FLOW3 1.0.0		
Subject:	Arguments of form __referrer are unserialized without a check		

Description

The request arguments of the referring request are a serialized string written to one of the hidden fields in a Fluid form. As the string is not checked before unserializing it, it is possible to unserialized arbitrary available objects.

Solution: This string has to be protected by a HMAC to protect FLOW3 from possible unserialize attacks.

Associated revisions

Revision cd39af5d - 2012-03-28 10:32 - Andreas Förthner

[SECURITY] Protect arguments of form __referrer with HMAC

The request arguments of the referring request are
a serialized string written to one of the hidden
fields in a Fluid form. This string has to be protected
by a HMAC to protect FLOW3 from possible unserialize
attacks.

Note: For now there is no object known within the FLOW3
Distribution, that could be used for an unserialize
exploit!

This change also backports some convenience hmac methods
to the hash service from the current master, to have the
bugfix in sync.

Change-Id: Ifeb87d0a85308f25cff2573a1ce2fc62dcd1e5fd
Security-Bulletin: FLOW3-SA-2012-001
Fixes: #35300
Releases: 1.0, 1.1

Revision dc464504 - 2012-04-11 16:12 - Andreas Förthner

[SECURITY] Protect arguments of form __referrer with HMAC

The request arguments of the referring request are
a serialized string written to one of the hidden
fields in a Fluid form. This string has to be protected
by a HMAC to protect FLOW3 from possible unserialize

attacks.

Note: For now there is no object known within the FLOW3
Distribution, that could be used for an unserialize
exploit!

Change-Id: I329f75052d2732f1baf4d26f6fd70cd9d009a65e
Security-Bulletin: FLOW3-SA-2012-001
Fixes: #35300
Releases: 1.0, 1.1

History

#1 - 2012-03-28 10:26 - Gerrit Code Review

- Status changed from New to Under Review

Patch set 3 for branch **FLOW3-1.0** has been pushed to the review server.
It is available at http://review.typo3.org/9897

#2 - 2012-03-28 10:29 - Bastian Waidelich

Shouldn't the target version be "Some version"? ;)

#3 - 2012-03-28 10:30 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9898

#4 - 2012-03-28 10:32 - Gerrit Code Review

Patch set 3 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9898

#5 - 2012-03-28 10:32 - Gerrit Code Review

Patch set 4 for branch **FLOW3-1.0** has been pushed to the review server.
It is available at http://review.typo3.org/9897

#6 - 2012-03-28 13:35 - Gerrit Code Review

Patch set 1 for branch **FLOW3-1.0** has been pushed to the review server.
It is available at http://review.typo3.org/9975

#7 - 2012-03-28 13:39 - Gerrit Code Review

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

It is available at http://review.typo3.org/9976

#8 - 2012-03-28 13:44 - Andreas Förthner

- Subject changed from some issue to Arguments of form __referrer are unserialized without a check

- Priority changed from Should have to Must have

- PHP Version set to 5.3

#9 - 2012-03-28 14:40 - Andreas Förthner

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:cd39af5dddd1695b499ca038c5add38d46436e4c.

#10 - 2012-04-11 16:05 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9976

#11 - 2012-04-11 16:11 - Gerrit Code Review

Patch set 3 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9976

#12 - 2012-04-11 16:12 - Gerrit Code Review

Patch set 4 for branch **master** has been pushed to the review server.
It is available at http://review.typo3.org/9976

#13 - 2012-04-15 02:39 - Andreas Förthner

- Status changed from Under Review to Resolved

Applied in changeset commit:dc46450431cf55667da03bfdd9c624291479d953.