TYPO3.Neos - Bug # 54592

Status:	Resolved	**Priority:**	Should have
Author:	Rens Admiraal	**Category:**	
Created:	2013-12-25	**Assigned To:**	
Updated:	2014-03-03	**Due date:**	
Subject:	Security policies are too strict		

Description

The following policy is far too strict:

```
TYPO3_Neos_AllControllerActions: 'within(TYPO3\Flow\Mvc\Controller\AbstractController) && method(public .*->.*Action())'
```

This secures all controllers in the full Flow application, which is an issue if you create an application in Flow and add Neos on top for managing a few content pages (or in whatever other usecase Flow packages would be used next to Neos).

I'm not sure if we want to secure all plugins of developers by default, or just want to secure all Neos controllers. But for now I would suggest only securing all controllers in the TYPO3\Neos\* namespace.

Associated revisions

Revision d05899f1 - 2014-03-03 20:43 - Rens Admiraal

[BUGFIX] Security policies in Neos are too strict

The current security policies fail with a "could not authenticate
any token" if an initializeAction is made public.

This change updates the policy so it does not match initialize
actions to prevent this error.

Change-Id: I167fc4effa0dba3e01599dbc114bc0d245aa17fc
Fixes: #54592
Releases: master, 1.0
Reviewed-on: https://review.typo3.org/26557
Reviewed-by: Andreas Förthner
Reviewed-by: Rens Admiraal
Tested-by: Rens Admiraal
Reviewed-by: Dominique Feyer
Tested-by: Dominique Feyer
Reviewed-by: Aske Ertmann
Reviewed-by: Christian Mueller
Tested-by: Christian Mueller

Revision 9578321c - 2014-03-03 20:47 - Rens Admiraal

[BUGFIX] Security policies in Neos are too strict

The current security policies fail with a "could not authenticate
any token" if an initializeAction is made public.

This change updates the policy so it does not match initialize
actions to prevent this error.

Change-Id: I167fc4effa0dba3e01599dbc114bc0d245aa17fc
Fixes: #54592
Releases: master, 1.0
Reviewed-on: https://review.typo3.org/28001
Reviewed-by: Christian Mueller
Tested-by: Christian Mueller
Reviewed-by: Rens Admiraal

History

#1 - 2013-12-25 00:47 - Gerrit Code Review

- Status changed from New to Under Review

Patch set 1 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/26557

#2 - 2013-12-26 01:12 - Rens Admiraal

Some extra clarification for the issue...

This policy is so general that it matches all controllers wherever in your installation, is it Flow or Neos, doesn't matter. I now have a project in which we can't add Neos because of this policy. Even this Policy.yaml does not allow access to the controller, and throws a 'context contained no tokens that could be authenticated':

```
resources:
  methods:
    My_Vendor_Controller: 'method(My\Vendor\.*Controller->.*Action())'

acls:
  Anonymous:
    methods:
      My_Vendor_Controller: GRANT
  Everybody:
    methods:
      My_Vendor_Controller: GRANT
```

This Policy.yaml does work fine if I disable the TYPO3_Neos_AllControllerActions resource (tested by adding a DENY)

#3 - 2013-12-27 17:09 - Gerrit Code Review

Patch set 2 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/26557

#4 - 2014-03-03 20:45 - Gerrit Code Review

Patch set 1 for branch **1.0** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/28001

#5 - 2014-03-03 21:36 - Rens Admiraal

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:9578321c3437e8e0d42a714d9631bc29a420f192.