ESUP-2011-AVI-001 - Vulnérabilité dans le plugin Cas de Nuxeo (esup-ecm)

Utilisation et diffusion de ce document

Objet :	Vulnérabilité dans le plugin CAS de Nuxeo
Référence :	ESUP-2011-AVI-001
Date :	25 novembre 2011
Pièces jointes	Fichiers jars correctifs
Détail	https://jira.nuxeo.com/browse/NXP-7882

Risque

When two users log in and retrieve a ticket from the CAS server at exactly the same time, they may end up with the other user's ticket (and so be logged in with its identity and rights).

This is due to the fact that in nuxeo's CAS2 plugin the authenticator implementation is not thread-safe.

Systèmes affectés

- Toutes les distributions du plugin CAS jusqu'à la version 5.5 SNAPSHOT incluse

Solution

Récupérer les jars incluant le correctif sur le site de Nuxeo ou téléchargez les plugins incluant le correctif + le patch pour le proxy CAS ici (attention, ces derniers sont en cours de validation et n'ont pu être complètement testés).

Plugin CAS pour la version 5.3.2 (esup-ecm 1.1.2)

Plugin CAS pour la version 5.4.1

Plugin CAS pour la version 5.4.2

Plugins délivrés par Nuxeo :

Version 5.3.2

Version 5.4.1 (et 5.4.0)

Version 5.4.2