Backlog Courrier - Fonctionnalité #9099

[ANALYSE] Etude des vulnérabilités PHP selon rapport ANSSI et impact Maarch Courrier

12/11/2018 09:42 AM - Emmanuel DILLARD

Status:	Développé / Analysé (S)	**Start date:**	12/11/2018
Priority:	1-Majeur	**Due date:**	
Assignee:	EDI PO		
Category:			
Target version:	19.04 (Sécurité)		
Tags Courrier:		**ROADMAP:**	

Description

Lien vers le rapport : https://www.cert.ssi.gouv.fr/avis/CERTFR-2018-AVI-588/

Demande SPM

History

#2 - 12/11/2018 12:27 PM - Emmanuel DILLARD

- Tracker changed from Anomalie to Fonctionnalité

- Project changed from Backlog to CURRENT SPRINT

- Status changed from Prêt à développer to En cours de dev (S)

#3 - 12/11/2018 02:21 PM - Emmanuel DILLARD

- Project changed from CURRENT SPRINT to Backlog

- Status changed from En cours de dev (S) to Développé / Analysé (S)

Voici notre analyse du problème :

1. vulnérabilité sur convert.quoted-printable-encode :
   Nous n'utilisons pas cette fonctionnalité dans nos produits.

2. vulnérabilité sur imap_open :
   Fonctionnalité utilisée pour l'envoi des mails dans MaarchCapture et pour contrôle des paramètres de MaarchCapture dans MaarchCourrier.
   Analyse :
   Le risque de l'exploitation de cette faille est peu élevé car il faudrait avoir accès à votre serveur Magec, et modifier les fichiers de paramétrage XML du module MailCapture de MaarchCapture pour y mettre du code permettant d'exécuter du code sur ce même serveur via la commande imap_open.
   On ne peut accéder à ces fichiers de paramétrages XML que si on a accès au serveur Magec. Ces fichiers sont hors du périmètre du service WEB.

Contournement en attendant d'installer php 5.6.39 :
Modifier le php.ini pour y ajouter les directives :
imap.set_rshtimeout=0
imap.set_sshtimeout=0
Cela devrait permettre d'éviter à PHP de lancer une commande de type RSH, la faille justement exploitée sur la commande imap_open pour lancer un exec sur le système hôte de PHP.

#6 - 06/09/2021 11:07 AM - Emmanuel DILLARD

- Project changed from Backlog to Backlog Courrier

- Target version changed from 19.04 (Support sécurité) to 19.04 (Sécurité)