Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 09 novembre 2010
N° CERTA-2010-AVI-542

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Novell GroupWise

Gestion du document

Référence	CERTA-2010-AVI-542
Titre	Vulnérabilités dans Novell GroupWise
Date de la première version	09 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Novell 7007151 à 7007159 du 08 novembre 2010
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

Novell GroupWise 8.

3 Résumé

Plusieurs vulnérabilités affectent Novell GroupWise 8. Les plus importantes permettent à un utilisateur distant non authentifié d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent Novell GroupWise 8 :

– des défauts dans les traitements des valeurs multiples, des chaînes de caractères et des nombres dans le

champ *Content-Type* des messages reçus permettent à un utilisateur distant non authentifié d'exécuter du code arbitraire à distance ;
- une erreur dans le composant IMAP permet à un utilisateur distant non authentifié d'exécuter du code arbitraire à distance, quand le service IMAP est activé ;
- une autre erreur dans ce composant permet à un utilisateur distant authentifié d'exécuter du code arbitraire à distance, quand le service IMAP est activé ;
- le composant WebPublisher permet à un utilisateur malveillant de réaliser de l'injection de code indirecte (XSS) ;
- l'interface HTTP des agents GroupWise présente un défaut qui permet à un utilisateur malveillant non authentifié d'exécuter du code arbitraire à distance ;
- une erreur dans GroupWise WebAccess Agent et Document Viewer Agent permet à un utilisateur distant non authentifié malveillant de récupérer n'importe quel fichier présent sur le serveur GroupWise WebAccess.

5 Solution

L'application du *Hot Patch* 8.02 remédie à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Novell 7007151 à 7007159 du 08 novembre 2010 :
  http://www.novell.com/support/viewContent.do?externalId=7007151
  http://www.novell.com/support/viewContent.do?externalId=7007152
  http://www.novell.com/support/viewContent.do?externalId=7007153
  http://www.novell.com/support/viewContent.do?externalId=7007154
  http://www.novell.com/support/viewContent.do?externalId=7007155
  http://www.novell.com/support/viewContent.do?externalId=7007156
  http://www.novell.com/support/viewContent.do?externalId=7007157
  http://www.novell.com/support/viewContent.do?externalId=7007158
  http://www.novell.com/support/viewContent.do?externalId=7007159

Gestion détaillée du document

09 novembre 2010 version initiale.