Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 février 2009
N° CERTA-2009-AVI-044

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Novell GroupWise

Gestion du document

Référence	CERTA-2009-AVI-044
Titre	Multiples vulnérabilités dans Novell GroupWise
Date de la première version	03 février 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Novell du 30 janvier 2009 Bulletins de sécurité Novell du 02 février 2009
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Novell GroupWise versions 6.x ;
- Novell GroupWise versions 7.x ;
- Novell GroupWise versions 8.x ;

3 Résumé

De multiples vulnérabilités ont été découvertes dans les différentes versions de `Novell GroupWise`. L'exploitation de ces vulnérabilités permet d'effectuer diverses actions malveillantes, dont l'exécution de code arbitraire à distance.

4 Description

Cinq vulnérabilités ont été découvertes dans les différentes versions de `Novell GroupWise`:

- la première vulnérabilité est due à un mauvais contrôle des valeurs passées aux paramètres *Userid* et *Library.queryText*. L'exploitation de cette vulnérabilité permet d'effectuer des attaques par injection de code indirecte ;
- la deuxième vulnérabilité est due à un mauvais contrôle du HTML contenu dans les mails. Cette vulnérabilité peut être exploitée afin d'effectuer des attaques par injection de code indirecte ;
- la troisième vulnérabilité est consécutive à un manque de contrôle des actions permises à l'utilisateur. Cette vulnérabilité peut être exploitée afin de contourner la politique de sécurité mise en place ;
- la quatrième vulnérabilité résulte d'un mauvais traitement des requêtes de type *POST*. Cette vulnérabilité peut être exploitée afin de contourner la politique de sécurité mise en place ;
- la dernière vulnérabilité résulte d'une erreur de type *off-by-one* dans le traitement de certaines requêtes HTTP. L'exploitation de cette vulnérabilité permet d'exécuter du code arbitraire à distance.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletins de mise à jour Novell GroupWise :
  http://www.novell.com/support/viewContent.do?externalId=7002319
  http://www.novell.com/support/viewContent.do?externalId=7002320
  http://www.novell.com/support/viewContent.do?externalId=7002321
  http://www.novell.com/support/viewContent.do?externalId=7002322
  http://www.novell.com/support/viewContent.do?externalId=7002502
- Référence CVE CVE-2009-0272 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0272
- Référence CVE CVE-2009-0273 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0273
- Référence CVE CVE-2009-0274 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0274

Gestion détaillée du document

03 février 2009 version initiale.