



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 septembre 2011
N° CERTA-2011-AVI-538

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Novell GroupWise

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-538>

Gestion du document

Référence	CERTA-2011-AVI-538
Titre	Multiples vulnérabilités dans Novell GroupWise
Date de la première version	29 septembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Novell du 26 septembre 2011
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 ;
- injection de code indirecte à distance.

2 Systèmes affectés

Novell GroupWise 8.0x jusqu'à la version 8.02HP2 (version comprise).

3 Résumé

De multiples vulnérabilités ont été identifiées dans les produits Novell GroupWise. Ces vulnérabilités peuvent notamment être utilisées pour réaliser de l'exécution de code arbitraire.

4 Description

De multiples vulnérabilités ont été corrigées dans les produits Novell GroupWise. Ces vulnérabilités peuvent être exploitées par une personne malintentionnée distante pour provoquer l'exécution de code arbitraire, de l'injection code indirecte (XSS), ou un déni de service.

5 Solution

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

6 Documentation

- Bulletin de sécurité Novell 7009208 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009208>
- Bulletin de sécurité Novell 7009210 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009210>
- Bulletin de sécurité Novell 7009214 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009214>
- Bulletin de sécurité Novell 7006378 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7006378>
- Bulletin de sécurité Novell 7009212 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009212>
- Bulletin de sécurité Novell 7009215 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009215>
- Bulletin de sécurité Novell 7009216 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009216>
- Bulletin de sécurité Novell 7009207 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009207>
- Bulletin de sécurité Novell 7009213 du 26 septembre 2011 :
<http://www.novell.com/support/viewContent.do?externalid=7009213>
- Référence CVE CVE-2010-4325 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4325>
- Référence CVE CVE-2011-0333 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0333>
- Référence CVE CVE-2011-0334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0334>
- Référence CVE CVE-2011-2218 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2218>
- Référence CVE CVE-2011-2219 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2219>
- Référence CVE CVE-2011-2661 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2661>
- Référence CVE CVE-2011-2662 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2662>
- Référence CVE CVE-2011-2663 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2663>

Gestion détaillée du document

29 septembre 2011 version initiale.