Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 avril 2011
N° CERTA-2011-AVI-261

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans MediaWiki

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-261

Gestion du document

Référence	CERTA-2011-AVI-261
Titre	Multiples vulnérabilités dans MediaWiki
Date de la première version	28 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de mise à jour MediaWiki versions 1.16.3 du 12 avril 2011 Bulletin de mise à jour MediaWiki 1.16.4 du 14 avril 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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

MediaWiki versions antérieures à 1.16.4.

3 Résumé

Plusieurs vulnérabilités ont été corrigés avec la version 1.16.3 de MediaWiki. Deux d'entre-elles permettent de réaliser de l'injection de code indirecte à distance.

4 Description

Trois vulnérabilités ont été corrigées :

- certains paramètres passés dans l'ajout de commentaires ne sont pas correctement validés, permettant à un attaquant de réaliser de l'injection de code indirecte (CVE-2011-1579) ;

– une fonction d'import ne vérifie pas correctement les permissions, autorisant une personne malveillante d'importer indument des ressources (CVE-2011-1580) ;
– il est possible de tromper certains navigateurs, comme Internet Explorer 6, et de leur faire interpréter certains fichiers comme du HTML, permettant à une personne malveillante de réaliser de l'injection de code indirecte (CVE-2011-1578).

Cette dernière vulnérabilité n'ayant pas été totalement corrigée avec la version 1.16.3 de MediaWiki, un nouveau correctif est disponible avec la version 1.16.4.

5 Solution

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

6 Documentation

– Bulletin de mise à jour MediaWiki versions 1.16.3 du 12 avril 2011 :
http://lists.wikimedia.org/pipermail/mediawiki-announce/2011-April/000096.html
– Bulletin de mise à jour MediaWiki versions 1.16.4 du 14 avril 2011 :
http://lists.wikimedia.org/pipermail/mediawiki-announce/2011-April/000097.html
– Référence CVE CVE-2011-1578 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1578
– Référence CVE CVE-2011-1579 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1579
– Référence CVE CVE-2011-1580 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1580

Gestion détaillée du document

28 avril 2011 version initiale.