Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 juin 2009
N° CERTA-2009-AVI-260

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Adaptive Security Appliance

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-2009-AVI-260

Gestion du document

Référence	CERTA-2009-AVI-260
Titre	Multiples vulnérabilités dans Cisco Adaptive Security Appliance
Date de la première version	30 juin 2009
Date de la dernière version	–
Source(s)	Bulletins d'alerte Cisco 18373, 18442 et 18536 du 24 juin 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

- Atteinte à la confidentialité des données ;
- injection de code indirecte.

2 Systèmes affectés

- Cisco ASA software versions antérieures à la 8.0.4(34) ;
- Cisco ASA software versions antérieures à la 8.1.2(25) ;
- Cisco ASA software versions antérieures à la 8.2.1(3).

Toutes ces versions sont vulnérables lorsqu'elles sont installées sur les équipements Cisco ASA 5505, 5510, 5520, 5540, 5550 et 5580.

3 Résumé

Plusieurs vulnérabilités affectant `Cisco ASA software` permettent à une personne malintentionnée de porter atteinte à la confidentialité des données et d'effectuer une injection de code indirecte.

4 Description

Plusieurs vulnérabilités ont été découvertes dans `Cisco ASA Software`:

- un manque de restriction à l'accès au *Document Object Model* (*DOM*) permet à une personne malintentionnée d'effectuer une injection de code indirecte ;
- un manque de contrôle sur le paramètre *Rot13-encoded* permet à une personne malintentionnée d'effectuer une injection de code indirecte ;
- un manque de contrôle et d'alerte lors de l'utilisation de *Common Internet File System* (*CIFS*) et des partages *FTP* permet à une personne malintentionnée de voler les données d'identification d'un utilisateur.

5 Solution

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

6 Documentation

- Bulletin d'alerte Cisco 18373 du 24 juin 2009 :
  http://tools.cisco.com/security/center/viewAlert.x?alertId=18373
- Bulletin d'alerte Cisco 18442 du 24 juin 2009 :
  http://tools.cisco.com/security/center/viewAlert.x?alertId=18442
- Bulletin d'alerte Cisco 18536 du 24 juin 2009 :
  http://tools.cisco.com/security/center/viewAlert.x?alertId=18536
- Référence CVE CVE-2009-1201 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1201
- Référence CVE CVE-2009-1202 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1202
- Référence CVE CVE-2009-1203 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1203

Gestion détaillée du document

30 juin 2009 version initiale.