Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 février 2012
N° CERTA-2012-AVI-096

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans CISCO SRP 500 Series

Gestion du document

Référence	CERTA-2012-AVI-096
Titre	Multiples vulnérabilités dans CISCO SRP 500 Series
Date de la première version	24 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20120223-srp500 du 23 février 2012
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.

2 Systèmes affectés

- CISCO SRP 521W avec microcode antérieur à 1.1.26 ;
- CISCO SRP 526W avec microcode antérieur à 1.1.26 ;
- CISCO SRP 527W avec microcode antérieur à 1.1.26 ;
- CISCO SRP 521W-U avec microcode antérieur à 1.2.4 ;
- CISCO SRP 526W-U avec microcode antérieur à 1.2.4 ;
- CISCO SRP 527W-U avec microcode antérieur à 1.2.4 ;
- CISCO SRP 541W avec microcode antérieur à 1.2.4 ;
- CISCO SRP 546W avec microcode antérieur à 1.2.4 ;
- CISCO SRP 547W avec microcode antérieur à 1.2.4.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans le microcode des équipements CISCO série SRP 500, qui peuvent être exploitées pour exécuter du code arbitraire à distance.

4 Description

Trois vulnérabilités ont été corrigées dans le microcode des équipements CISCO série SRP 500. Elles peuvent être exploitées par un attaquant via l'interface réseau local (LAN) en configuration par défaut, ou via l'interface réseau étendu (WAN) si l'administration distante est autorisée. Ces exploitations permettent 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

- Bulletin de sécurité Cisco 20120223-srp500 du 23 février 2012 :
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120223-srp500
- Référence CVE CVE-2012-0363 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0363
- Référence CVE CVE-2012-0364 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0364
- Référence CVE CVE-2012-0365 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0365

Gestion détaillée du document

24 février 2012 version initiale.