

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans les produits Cisco

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTFR-2015-AVI-505 |
| Titre | Vulnérabilité dans les produits Cisco |
| Date de la première version | 26 novembre 2015 |
| Date de la dernière version | - |
| Source(s) | Bulletin de sécurité Cisco cisco-sa-20151125-ci du 25 novembre 2015 |
| 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(s)

- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco RV320 Dual Gigabit WAN VPN Router
- Cisco RV325 Dual Gigabit WAN VPN Router
- Cisco RV325 Dual WAN Gigabit VPN Router
- Cisco RVS4000 4-port Gigabit Security Router - VPN
- Cisco WRV210 Wireless-G VPN Router - RangeBooster
- Cisco WAP4410N Wireless-N Access Point - PoE/Advanced Security
- Cisco WRV200 Wireless-G VPN Router - RangeBooster
- Cisco WRVS4400N Wireless-N Gigabit Security Router - VPN V2.0
- Cisco WAP200 Wireless-G Access Point - PoE/Rangebooster
- Cisco WVC2300 Wireless-G Business Internet Video Camera - Audio
- Cisco PVC2300 Business Internet Video Camera - Audio/PoE
- Cisco SRW224P 24-port 10/100 + 2-port Gigabit Switch - WebView/PoE
- Cisco WET200 Wireless-G Business Ethernet Bridge
- Cisco WAP2000 Wireless-G Access Point - PoE
- Cisco WAP4400N Wireless-N Access Point - PoE
- Cisco RV120W Wireless-N VPN Firewall

- Cisco RV180 VPN Router
- Cisco RV180W Wireless-N Multifunction VPN Router
- Cisco RV315W Wireless-N VPN Router
- Cisco Small Business SRP520 Models
- Cisco Small Business SRP520-U Models
- Cisco WRP500 Wireless-AC Broadband Router with 2 Phone Ports
- Cisco SPA400 Internet Telephony Gateway with 4 FXO Ports
- Cisco RTP300 Broadband Router
- Cisco RV220W Wireless Network Security Firewall

3 - Résumé

Une vulnérabilité a été corrigée dans les produits *Cisco*. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Cisco cisco-sa-20151125-ci du 25 novembre 2015
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-ci>
- Référence CVE CVE-2015-6358
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6358>

Gestion détaillée du document

26 novembre 2015 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-505>
