



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2008
N° CERTA-2008-AVI-489

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Unity

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-2008-AVI-489>

Gestion du document

Référence	CERTA-2008-AVI-489
Titre	Multiples vulnérabilités dans Cisco Unity
Date de la première version	10 octobre 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Cisco #108036 et #107983
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

- Déni de service ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco Unity 4.x ;
- Cisco Unity 5.x ;
- Cisco Unity 7.x.

3 Résumé

Plusieurs vulnérabilités dans les produits Cisco Unity permettent à un utilisateur distant de provoquer un déni de service, de contourner la politique de sécurité ou de porter atteinte à la confidentialité de certaines données.

4 Description

Plusieurs vulnérabilités sont présentes dans les produits Cisco Unity :

- la première concerne le processus d'authentification auprès du serveur Cisco Unity. Elle permet à un utilisateur malintentionné de contourner cette authentification pour accéder à certaines parties de la configuration du serveur ;
- la seconde est relative à la gestion des sessions ouvertes sur le serveur et permet à un utilisateur distant de provoquer un déni de service en consommant toutes les sessions disponibles ;
- la dernière concerne un mauvais positionnement de permissions sur un répertoire du serveur. Celle-ci permet à un utilisateur malintentionné du domaine de porter atteinte à certaines informations sensibles du système.

Les deux premières vulnérabilités ne sont exploitables que si le serveur Cisco Unity est configuré pour accepter les authentifications anonymes. Ce qui n'est pas le cas par défaut.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco ID 108036 du 08 octobre 2008 :
<http://www.cisco.com/warp/public/707/cisco-sa-20081008-unity.shtml>
- Bulletin de sécurité Cisco ID 107983 du 08 octobre 2008 :
<http://www.cisco.com/warp/public/707/cisco-sr-20081008-unity.shtml>
- Référence CVE CVE-2008-3814 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3814>

Gestion détaillée du document

10 octobre 2008 version initiale.