



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 juillet 2007
N° CERTA-2007-AVI-298-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 3Com TippingPoint IPS

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-2007-AVI-298>

Gestion du document

Référence	CERTA-2007-AVI-298-001
Titre	Vulnérabilité dans 3Com TippingPoint IPS
Date de la première version	11 juillet 2007
Date de la dernière version	12 juillet 2007
Source(s)	Alerte de sécurité 3COM-07-002 du 10 juillet 2007
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.

2 Systèmes affectés

- les produits 3Com TippingPoint IPS ayant une version TOS 2.1.x ;
- les produits 3Com TippingPoint IPS ayant une version TOS 2.2.x antérieure à 2.2.5 ;
- les produits 3Com TippingPoint IPS ayant une version TOS 2.5.x antérieure à 2.5.2.

3 Résumé

Une vulnérabilité a été identifiée dans le système d'exploitation TOS intégré aux solutions de sécurité 3Com TippingPoint IPS. Une fragmentation de paquets particulière permettrait de contourner la politique de détection mise en place.

4 Description

Une vulnérabilité a été identifiée dans le système d'exploitation TOS intégré aux solutions de sécurité 3Com TippingPoint IPS. Le service de détection ne fonctionnerait pas correctement sous certaines conditions de fragmentation des trames réseau (IP). L'exploitation de cette vulnérabilité permet ainsi à une personne malveillante distante de contourner les politiques de filtrage et de détection mises en place.

5 Solution

Se référer à l'alerte de sécurité l'éditeur 3Com pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Alerte 3Com 3COM-07-002 du 10 juillet 2007, « TippingPoint IPS Filter Bypass Vulnerability » :
<http://www.3com.com/securityalert/alerts/3COM-07-002.html>
- Avis de sécurité Cybsec du 04 juillet 2007 :
http://www.cybsec.com/vuln/CYBSEC-Security_Pre-Advisory_3Com_TippingPoint_IPS_Detection_Bypass_2.pdf
- Référence CVE CVE-2007-3711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3711>

Gestion détaillée du document

11 juillet 2007 version initiale.

12 juillet 2007 ajout de la référence CVE associée.