Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2001
N° CERTA-2001-AVI-094

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Attaques non détectées par certains IDS

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-2001-AVI-094

Gestion du document

Référence	CERTA-2001-AVI-094
Titre	Attaques non détectées par certains IDS
Date de la première version	13 septembre 2001
Date de la dernière version	–
Source(s)	Avis L139 du CIAC
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

Possibilité d'obtention de faux négatifs sur certains IDS.

2 Systèmes affectés

Les logiciels de détection d'intrusions suivant :

- CISCO NetRanger ;
- le module de détection d'intrusions des routeurs Catalyst 6000 ;
- Dragon sensor 4.x ;
- ISS realsecure Network Sensor 5.x, 6.x, avant XPU 3.2 et Server Sensor 6.0 et 5.5 pour Windows ;
- les versions de snort antérieures à la version 1.8.1.

Il est possible que d'autres systèmes de détection d'intrusions soient sensibles à cette vulnérabilité, contactez le distributeur de votre système.

3 Résumé

Certains IDS peuvent être leurrés par des codes malicieux utilisant un format `unicode` particulier.

4 Description

Certains IDS (*Intrusion Detection System* ou Système de Détection d'Intrusions) utilisent des « signatures » basées sur la recherche de chaines de caractères dans les paquets qui transitent sur le réseau afin de détecter l'occurence d'une attaque.

Un utilisateur mal intentionné peut créer un code malicieux utilisant un codage unicode particulier (que seuls les serveurs web Internet Information Server utilisent) dans une requête HTTP afin de tromper les IDS.

5 Solution

Appliquer les correctifs selon les systèmes :

- Cisco Secure Intrusion Detection System Sensor :
  ftp://ftp-eng.cisco.com/csids-sig-updates/ServicePacks/IDSK9-sp3.0-1.43-s6-0.43-bin
- Pour les autres produits CISCO, il faut avoir un contrat de maintenance :
  http://www.cisco.com
- Tous les produits ISS :
  http://www.iss.net/eval/eval.php
- Realsecure Network Sensor :
  http://www.iss.net/db_data/xpu/RS.php

6 Documentation

- L'avis L-139 du CIAC :
  http://www.ciac.org/ciac/bulletins/l-139.shtml
- L'avis Cisco :
  http://www.cisco.com/warp/public/707/cisco-intrusion-detection-obfuscation-vuln-pub.shtml

Gestion détaillée du document

13 septembre 2001 version initiale.