

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des équipements et applications CISCO sous SOLARIS

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-2002-AVI-076>

Gestion du document

Référence	CERTA-2002-AVI-076
Titre	Vulnérabilité des équipements et applications CISCO sous SOLARIS
Date de la première version	11 avril 2002
Date de la dernière version	03 juin 2002
Source(s)	Bulletin de sécurité CISCO "Solaris /bin/login Vulnerability"
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

- Elévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

- Cisco Media Gateway Controller (MGC) et les produits liés ;
- Cisco IDS.

Se référer à l'avis Cisco afin d'obtenir la liste des produits affectés (cf. Documentation).

3 Résumé

Vulnérabilité des produits Cisco installés sur une plate-forme Solaris.

4 Description

Les produits Cisco installés sur une plate-forme Solaris peuvent être affectés par la vulnérabilité de Solaris /bin/login (cf. Avis CERTA-2001-AVI-161) si aucun correctif n'a été appliqué. Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire.

Cisco a émit un avis sur cette vulnérabilité afin de rappeler la nécessité d'appliquer le correctif, cette vulnérabilité étant couramment exploitée.

5 Solution

Appliquer le correctif fournit par Sun selon les versions affectées:

<http://sunsolve.sun.com/securitypatch>

6 Documentation

Bulletin de sécurité Cisco "Solaris /bin/login Vulnerability" :

<http://www.cisco.com/warp/public/707/Solaris-bin-login.shtml>

Gestion détaillée du document

11 avril 2002 version initiale.

03 juin 2002 correction du lien vers le bulletin CISCO.