Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 octobre 2001
N° CERTA-2001-AVI-105

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les agents de supervision Compaq

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-105

Gestion du document

Référence	CERTA-2001-AVI-105
Titre	Vulnérabilité dans les agents de supervision Compaq
Date de la première version	01 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité SSRT0758 de Compaq
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 ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

Les agents de supervision Compaq sont utilisés sur de nombreuses plate-formes du constructeur.
La liste des systèmes affectés est disponible sur le site de Compaq :
http://www.compaq.com/products/servers/management/mgtsw-advisory2.html

3 Résumé

Un utilisateur mal intentionné peut utiliser une vulnérabilité dans les agents de supervision Compaq interrogeables via HTTP pour exécuter du code arbitraire à distance avec les privilèges de l'administrateur.

4 Description

Les agents de supervision Compaq sont utilisés sur les équipements de ce constructeur.

Une vulnérabilité de type débordement de mémoire dans les agents d'administration accessibles via HTTP permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de l'administrateur.

5 Contournement provisoire

Compaq rappelle que ce type de service ne devrait pas être accessible en dehors du réseau interne.

Il convient donc de bloquer l'accès au port 2301 au niveau des routeurs périphériques ou des pare-feux, rendant ainsi la vulnérabilité exploitable uniquement depuis le réseau interne.

6 Solution

Une mise-à-jour est disponible sur le site Compaq :
ftp://ftp.compaq.com/pub/softpaq/sp17501-1800/

7 Documentation

Avis de sécurité SSRT0758 de Compaq :
http://www.compaq.com/products/servers/management/mgtsw-advisory.html

Gestion détaillée du document

01 octobre 2001 version initiale.