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 février 2001
N° CERTA-2001-AVI-016

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des logiciels d'administration à distance de Compaq

Gestion du document

Référence	CERTA-2001-AVI-016
Titre	Vulnérabilité des logiciels d'administration à distance de Compaq
Date de la première version	12 février 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Compaq Avis 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

- Déni de service;
- exécution de code arbitraire à distance avec des privilèges élevés.

2 Systèmes affectés

Le risque affecte la plupart des machines Compaq (voir le paragraphe 'description') indépendamment du système d'exploitation.

3 Résumé

Une vulnérabilité du logiciel d'administration à distance du matériel Compaq avec interface HTML permet à un utilisateur mal intentionné de compromettre une machine indépendamment du système d'exploitation qui y est installé.

4 Description

Les agents d'administration Compaq avec une interface de présentation en HTML (*web-enabled Management Agent*) permettent une administration centralisée du matériel informatique de la marque Compaq (mettre à jour les pilotes de périphériques, lister le matériel, démarrer ou arrêter les cartes réseau, etc.) en s'appuyant sur un serveur web.

Une vulnérabilité de ce logiciel permet, si l'interface de présentation en HTML est activée sur la machine cible, d'exécuter à distance du code avec des privilèges élevés (par exemple : `Local System` sous Windows NT).

L'interface web est activée par défaut sur les systèmes Windows.

5 Contournement provisoire

Désactiver l'interface HTML de l'agent d'administration à distance.

- Pour l'agent d'administration (*Management agent*) Sous Windows :
  Dans le « Menu Démarrer », choisir « Paramètres », puis « Panneau Configuration », double-cliquer sur « Services » Dans la liste des services choisir « INSIGHT WEB AGENT » et cliquer sur le bouton « Arrêter » si le service est en marche. Et pour l'empêcher de redémarrer automatiquement ultérieurement, cliquer sur le bouton « Démarrage » puis « Manuel ». Cliquer sur « OK » puis « Fermer ».
- Pour les stations et portables sous Windows, il faut désinstaller l'agent web (*web-enabled Agent*) pour le réinstaller avec l'option « DMI web agent » en moins.
  Dans le panneau configuration choisir « ajout/suppression de programmes ». Après avoir sélectionné Compaq Insight Management Web Agent », cliquer sur le bouton « ajouter/supprimer ».
  Puis réinstaller le logiciel.
  - Pour les stations de travail : ne pas cocher la case « DMI Web Components » pendant l'installation.
  - Pour les portables, pendant l'installation, il faut choisir « Custom » (pour « personnaliser »), puis choisir « DMI options » et cliquer sur le bouton « Change ». Décocher les options « Compaq DMI Web Agent » et « Compaq DMI Web Viewer ».
- Pour l'agent d'administration sous Netware :
  Démarrer le programme « `CPQAGIN` ». Choisir l'option « Configurer un Agent Netware existant ». Sur la ligne mentionnant le chargement de « `CPQWEBAG` » sélectionner « NON ». Enregistrer et sortir du programme « `CPQAGIN` ».
- Pour l'agent d'administration sous Linux :
  Se connecter comme `root`, et lancer
  `/etc/rc.d/init.d/cmafdtn` pour arrêter le démon `cmawebd`.
  Pour l'empêcher de redémarrer automatiquement ultérieurement, éditer le fichier
  `/etc/rc.d/init.d/cmafdtn`
  et supprimer `cmawebd` de la ligne :
  `PNAMES="cmafdtnpeerd wmhostd cmathreshd cmawebd`.
- Pour l'agent d'administration sous SCO UnixWare 7 :
  Se connecter comme `root`, et lancer :
  `sh /etc/init.d/cmafdtn stop` pour arrêter le démon `cmawebd`.
  Pour l'empêcher de redémarrer automatiquement ultérieurement, détruire ou plutôt déplacer ou renommer le fichier :
  `/etc/rc2.d/[SK]*cmafdtn`.
- Pour l'agent d'administration sous SCO OpenWare :
  Se connecter comme `root`, et lancer :
  `sh /etc/cmafdtn stop` pour arrêter le démon `cmawebd`.
  Pour l'empêcher de redémarrer automatiquement ultérieurement, détruire ou plutôt déplacer ou renommer le fichier
  `/etc/rc2.d/[SK]*cmafdtn`.
- Pour le logiciel *Survey* sous Windows :
  Passer sous l'invite de commande, et taper :
  `%systemdrive%\COMPAQ\SURVEY\SURVEY-U`.
  Ceci arrête le service Survey et l'empêchera de redémarrer à l'avenir.

- Pour le logiciel *Survey* sous Netware :
  Passer sous l'invite de commande, et taper :
  `UNLOAD SURVEY`.
  Pour qu'il ne redémarre pas ultérieurement, supprimer la ligne :
  `load SURVEY -w10 -cWed.12,7` du fichier *AUTOEXEC.NCF*.
- Pour l'agent d'administration sous OpenVMS :
  Se connecter au compte système, et taper la commande suivante :
  - Pour les versions 1.0 et 2.0 : `$@sys$specific:[wbem]stop webagents`
  - Pour la version 2.1 : `$@sys$specific:[wbem]wbem$shutdown`
- Pour l'agent d'administration sous Tru64 Unix :
  Se connecter comme `root`, et exécuter la commande suivante :
  `/sbin/init.d/insightd stop` pour arrêter le service.
  Afin empêcher le serveur de redémarrer :
  - Pour les version 4.0f et 4.0g supprimer le fichier `/sbin/rc2.d/*insightd`.
    Il pourra être redémarré après application du correctif par la commande :
    `ln -s /sbin/init.d/insightd/sbin/rc2.d/kxxinsightd`
    où les 'x' représentent n'importe quelle séquence de nombres supérieure à celle utilisée pour snmpd.
  - pour les versions 5.0 et supérieures taper la commande :
    `/usr/bin/rcmgr set INSIGHTD_CONF -1`
    Il pourra être redémarré après application du correctif par la commande :
    `/usr/sbin/rcmgr set INSIGHTD_CONF 1`
- Pour désinstaller le « web-enabled Agent » de Tru64 :
  En tant que `root` taper la commande suivante :
  `/sbin/init.d/insightd stop`.
- Pour le logiciel *Healthcheck* :
  Aller dans le répertoire des binaires de SHC (par exemple : `cd \%systemdrive\%\compaq\shc\bin`), arrêter le service en tapant :
  `net stop cpqshc`, puis supprimer le service en tapant :
  `shcsvc -remove`.
  `Nota` : L'interface de commande de SHC fonctionnera toujours après la suppression du service.
- Pour Compaq Power Agent :
  Arrêter l'agent web : dans le « Panneau Configuration » double-cliquer sur « Services » dans la liste des services, sélectionner « Compaq Power Agent », et cliquer sur le bouton « arrêter ».
  Pour l'empêcher de redémarrer à l'avenir : cliquer sur le bouton « Démarrage » et choisir « Désactivé ».
- Pour Compaq Management Agent et ses outils pour SCO UnixWare NonStop Cluster :
  Se connecter avec le compte `root`, puis exécuter les commandes :
  `onall /etc/init.d/cmaweb stop` et
  `chmod 777 /etc/init.d/cmaweb 000`

6 Solution

Appliquer selon les cas rencontrés les correctifs indiqués sur l'avis de Compaq:
http://www5.compaq.com/products/servers/management/agentsecurity.html

7 Documentation

- Bulletin de sécurité de Compaq :
  http://www5.compaq.com/products/servers/management/agentsecurity.html
- avis de sécurité du CIAC :
  http://www.ciac.org/ciac/bulletins/l-042.shtml

Gestion détaillée du document

12 février 2001 version initiale.