



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 décembre 2007  
N° CERTA-2007-AVI-556

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans HP Quick Launch Button (QLB)

---

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-556>

---

### Gestion du document

Référence	CERTA-2007-AVI-556
Titre	Multiples vulnérabilités dans HP Quick Launch Button (QLB)
Date de la première version	19 décembre 2007
Date de la dernière version	–
Source(s)	Annonce de sécurité HP sp38166 du 12 décembre 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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

HP Quick Launch Button (QLB) est installé par défaut sur plusieurs modèles de portables de type *Notebooks*, dont :

- la famille des Compaq Presario Notebook PC Series (A900, B1200, C500, C700, F500, F700, M2000, V2000, V3000, V3500, V3700, V4000, V6500 et V6700) ;
- la famille des HP Notebook PC (500, 510, 520, 530, G5000, G6000, G7000 et Special Edition L2000) ;
- la famille des HP Compaq Notebook PC (2210b, 2510p, 2710p, 6510b, 6515b, 6520s, 6710b, 6710s, 6715b, 6715s, 6720s, 6820s, 6910p, 8510p, 8510w, 8710p, 8710w, nc2400, nc4200, nc4400, nc6110, nc6120, nc6140, nc6220, nc6320, nc6400, nc8230, nc8430, nw8240, nw8440, nw9440, nw4820, nx6110, nx6115, nx6120, nx6125, nx6310, nx6315, nx6320, nx6325, nx7300, nx7400, nx8220, nx8420 et nx9420) ;
- la famille des HP Compaq Tablet PC (tc4200 et tc4400) ;
- la famille des HP Pavillon Notebook PC Series (dv1000, dv2000, dv2500, dv2700, dv4000, dv6500, dv6700, dv9500, dv9700, dx6500, HDX, tx1000 et ze2000).

### 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le logiciel HP Quick Launch Button (QLB) servant notamment à gérer les raccourcis de certaines touches. Il est installé par défaut sur la majorité des portables HP et Compaq de type *Notebook* équipés de Microsoft Windows (2000, XP et Vista).

Ces vulnérabilités peuvent être exploitées par une personne malveillante distante, par exemple par le biais d'une page web spécialement construite, pour exécuter des applications arbitraires ou lire et modifier les valeurs du registre de la machine vulnérable.

### 4 Description

Plusieurs vulnérabilités ont été identifiées dans le logiciel HP Quick Launch Button (QLB) servant notamment à gérer les raccourcis de certaines touches. Il est installé par défaut sur la majorité des portables HP et Compaq de type *Notebook* équipés de Microsoft Windows (2000, XP et Vista).

Ces vulnérabilités concernent en particulier le contrôle ActiveX `HPInfoDLL.HPInfo.1` de `HPInfoDLL.dll` 1.0 fourni avec l'application *HP Info Center* (`hpinfocenter.exe`).

Elles peuvent être exploitées par une personne malveillante distante pour exécuter des applications arbitraires ou lire et modifier les valeurs du registre de la machine vulnérable par les méthodes `SetRegValue` et `GetRegValue`.

La désinstallation de l'application HP Quick Launch Button (QLB) n'est pas suffisante pour corriger le problème.

### 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

### 6 Documentation

- Annonce de sécurité HP sp38166 du 12 décembre 2007 :  
<ftp://ftp.hp.com/pub/sotfpaq/sp38001-38500/sp38166.html>
- Annonce de sécurité HP de référence HPSBGN02298 SSRT071502 rev.1 du 14 décembre 2007 :  
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01300486>
- Référence CVE CVE-2007-6331 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6331>
- Référence CVE CVE-2007-6332 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6332>
- Référence CVE CVE-2007-6333 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6333>

### Gestion détaillée du document

19 décembre 2007 version initiale.