ALERTE

Des PC Lenovo exposés à des risques de sécurité élevés

Systèmes affectés

Lenovo Notebook

- *Flex 2 Pro 15 (Broadwell)*
- *Flex 2 Pro 15 (Haswell)*
- *Flex 3 1120*
- *Flex 3 1470/1570*
- *G40-80/G50-80/G50-80 Touch*
- *S41-70/U41-70*
- *S435/M40-35*
- *V3000*
- *Y40-80*
- *Yoga 3 11*
- *Yoga 3 14*
- *Z41-70/Z51-70*
- *Z70-80/G70-80*

Lenovo Desktop
World Wide

- *A540/A740*
- *B750*
- *B4030 - 5035*
- *H3000 - 5055*
- *Horizon 2 27*
- *Horizon 2e(Yoga Home 500)*
- *Horizon 2S*
- *C260 - 5030*
- *X310(A78)*
- *X315(B85)*

Lenovo Desktop
China Only

- *D3000 - 5055*
- *F5000 - 5055*
- *G5000 - 5055*
- *YT A5700k*

- *YT A7700k*
- *YT M2620n*
- *YT M5310n*
- *YT M5790n*
- *YT M7100n*
- *YT S4005 - 5030*

Aperçu

Des vulnérabilités ont été découvertes dans le Lenovo Service Engine (LSE), module implanté directement dans le Bios des PC Lenovo dans le but d'aider les utilisateurs.

Lenovo a publié une mise à jour du BIOS pour désactiver le LSE et un utilitaire pour supprimer les services et les fichiers laissés sur le système pour les systèmes fonctionnant sous Windows 7, 8, 8.1 et 10.

Description

Le **Lenovo Service Engine** (LSE), installé directement au sein du Bios des PC du constructeur, altérait en effet les fichiers système de Windows afin de **forcer l'installation** de OneKey Optimizer, chargé d'assurer la mise en place des pilotes et applications proposés par Lenovo. Par la même occasion, des données 'anonymes' étaient remontées sur les serveurs de la société.

Lenovo, Microsoft et un chercheur indépendant ont découvert des failles dans ce programme qu'un attaquant pourrait exploiter pour commettre des attaques de type buffer overflow y compris une tentative de connexion à un serveur de test Lenovo.

Impact

Cette faille permet potentiellement l'installation de *malwares* à distance par des pirates. En effet un attaquant peut provoquer un buffer-overflow dans le LSE pour obtenir un accès administrateur au lancement de Windows, et ainsi être capable, par exemple, d'installer un rootkit qui donnera accès à l'ensemble du système à distance.

Solution

LENOVO a publié fin juillet un correctif (pour portables et pour ordinateurs de bureau) pour que ceux qui avaient déjà acheté l'un des ordinateurs concernés puissent supprimer LSE et ainsi se mettre à l'abri.

Références

- Bulletin de sécurité Lenovo : LEN-2015-020
- Lenovo Service Engine (LSE) BIOS Vulnerability : US-CERT
- SC Magazine

Révisions

- 25 aout 2015 – *Date de première publication*

Retour haut de page

Computer Incidents Response Team (CIRT)
01 BP 6437 Ouagadougou 01
Tel : +226 25 37 53 60/61/62 Poste 284 – Fax : +226 25 37 53 64 – Email : cirt(at)cirt.bf –
Signalement d'incidents : incidents(at)cirt.bf
Site Web : http://www.cirt.bf