Des failles critiques affectent les logiciels embarqués des stations Dell

Des failles critiques affectent des logiciels Dell préinstallé sur certains systèmes du constructeur. Sont concernés l'anti-malware Invincea-X, la solution de protection des terminaux Invincea Dell Protected Workspace et Dell Precision Optimizer, une solution d'optimisation des stations de travail. *« Les vulnérabilités présentes dans ces applications pourraient permettre aux attaquants de désactiver les mécanismes de sécurité, d'accroître les privilèges et d'exécuter du code arbitraire dans le contexte applicatif de l'utilisateur »*, alerte Talos, la division de veille sécuritaire de Cisco.

Selon le chercheur en sécurité Marcin 'Icewall' Noga, un risque d'accès à des privilèges administrateur affecte le pilote SboxDrv.sys. Référencée CVE-2016-9038, la vulnérabilité se déclenche par l'envoi de données spécialement conçues dans \Device\SandboxDriverApi. *« Une exploitation réussie entraîne l'écriture d'une valeur arbitraire dans l'espace mémoire du noyau, ce qui peut entraîner une escalade des privilèges locaux »*, indique le chercheur dans sa publication. Sont affectés Invincea-X et Dell Protected Workspace 6.1.3-24058.

Une DLL non vérifiée

Protected Workspace est également touché par une brèche (CVE-2016-8732) du composant InvProtectDrv.sys inclus dans la version 5.1.1-22303. Face aux restrictions limitées des canaux de communication du driver et de faibles systèmes de validation, une application contrôlée par un attaquant pourrait exploiter le pilote pour désactiver certains des mécanismes de protection du logiciel. Dell a apporté un correctif dans sa mise à jour 6.3.0.

Enfin, au démarrage du service Dell PPO de l'application Dell Precision Optimizer, le système charge par défaut le fichier atiadlxx.dll. Une bibliothèque qui peut-être remplacée alors qu'aucune vérification de signature n'est effectuée pour s'assurer de son intégrité. La encore, *« cela peut conduire à l'exécution d'un code arbitraire si un attaquant fournit une DLL malveillante du même nom »*, souligne Talos. Les Dell Precision Tower 5810 sont potentiellement affectés. Là aussi, Dell a réalisé un correctif sous forme d'une nouvelle version de son logiciel d'optimisation (disponible à partir de cette page).

Corriger ou supprimer

Il est paradoxal de constater que des logiciels de sécurité peuvent remettre en cause l'intégrité d'un système. En conséquence, Talos recommande aux utilisateurs d'appliquer les correctifs au plus vite. Ou de les désinstaller s'ils ne sont pas utilisés. *« Comme pour tout logiciel inutilisé, son élimination supprime les vulnérabilités associées et élimine le paquet supplémentaire des programmes de correctifs »*, rappelle Icewall plein de bon sens.

Lire également

Stockage : le règne de Dell Technologies débute dans la morosité
Dell sera le seul constructeur à proposer des PC AMD Theadripper en 2017
Dell-EMC : PowerEdge 14G, les serveurs automatisés pour la performance

crédit photo © drx – Fotolia.com