

4.4.5.2

Fonctionnalités

- Nouvelle télémétrie d'accès au niveau du noyau pour les comportements réseau, afin de mieux identifier les bugs réseau possibles côté client, ou les opportunités d'optimisation
- La télémétrie sortante est désormais regroupée et envoyée ensemble, tout comme les paramètres entrants
 - Transmise avec une variance de synchronisation de 25 %, afin que chaque machine n'envoie pas de paquets simultanément sur un réseau client
- HTTP/2 est désormais pleinement utilisé de bout en bout

Corrections

- Réduction du nombre minimum de threads utilisés en espace utilisateur
- Réduction de l'utilisation du CPU pour le service en espace utilisateur
- L'authentification Agent-Serveur est désormais effectuée plus efficacement
- Remplacement de l'ancien algorithme de mise en veille/redémarrage du service lorsque les licences n'étaient pas disponibles.
 - L'ancien algorithme provoquait un « service exited unexpectedly » (service arrêté de manière inattendue) dans le gestionnaire d'événements toutes les 15 minutes.
 - Permettre au système d'exploitation d'indiquer au service de s'arrêter (une pratique exploitée par des criminels et d'autres outils de sécurité) aurait permis un redémarrage « propre » du service sans journaux dans le gestionnaire d'événements. Plutôt que de créer cette vulnérabilité, le service de Cyber Crucible s'est redémarré lui-même sans l'intervention de Windows, ce qui génère l'entrée dans le journal d'événements.

Empreintes MD5

```
service.exe = b17a2a528a4424771fdeca8559b9f56b
CCRRSecMon.sys (Windows7) = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8) = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10) = 0d1fc32fba2cb878ce8cb0f549b8d167
```

