4.4.8.1

Fonctionnalités

- Les métadonnées des exécutables telles que la version du produit, le nom de la société, etc. pour les processus en mémoire sont signalées par le pilote via la visibilité du noyau. Le fonctionnement normal consiste à utiliser des appels API Windows en espace utilisateur. Ce passage à l'analyse au niveau du noyau supprime la possibilité (observée) pour les attaquants de falsifier les informations relatives aux processus.
- Les informations d'authentification de l'agent sont répliquées ailleurs dans le système afin de permettre une restauration en cas de corruption du registre par un pilote malveillant.

Améliorations

- Les erreurs de connexion au serveur sont enregistrées de manière minimale par l'agent, ce qui réduit la taille des journaux sur le disque.

Corrections

- N/A

Hachages MD5

```
service.exe  = 8c1f6999ccd176193e493686216f14c6
CCRRSecMon.sys (Windows7)        = 3b032d0e43674509126c6cb1c9efd688
CCRRSecMon.sys (Windows8)        = d3131131c83c2cf833ebc2157149c364
CCRRSecMon.sys (Windows10)       = eac8a8b38a8743a13dd7130509de9907
```

Revision #1
Created 2026-07-24 06:33:15 UTC by Dennis Underwood
Updated 2026-07-24 06:33:15 UTC by Dennis Underwood