4.4.1.0

Fonctionnalités

- Prise en charge étendue de l'analyse des injections de processus, afin d'augmenter considérablement la précision de la détection des intentions malveillantes ou bénignes pour les applications.
  - Cela est devenu particulièrement important en raison d'un petit nombre (<0,02 %) de machines dans la télémétrie de Cyber Crucible déclenchant des alertes sur des comportements agressifs d'injection de processus provenant de processus système.
- Capacité de surveillance accrue des processus système non signés.
  - Cela répond en partie à la forte concentration des attaquants sur l'implication de ces processus lors des opérations de mouvement latéral (sur un système, et entre les systèmes).

Corrections

- Modification d'un comportement de modification de fichier afin de réduire les faux positifs en ne déclenchant plus d'alerte sur certaines actions bénignes, grâce à un contexte supplémentaire au niveau du noyau concernant les comportements d'accès aux fichiers d'un processus.

Statut de validation WHCP/WHQL

Validé.

Empreintes MD5

```
service.exe   = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)       = 452719399d9bb98dc6b14fb8787d8415
```

```
CCRRSecMon.sys (Windows8)        = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)        = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

Revision #1
Created 2026-07-24 06:26:41 UTC by Dennis Underwood
Updated 2026-07-24 06:26:42 UTC by Dennis Underwood