4.4.1.0

Funciones

- Soporte ampliado para el análisis de inyección de procesos, con el fin de aumentar drásticamente la precisión en la detección de intención maliciosa frente a benigna en aplicaciones.
  - Esto se volvió especialmente importante debido a que un pequeño número (<0.02%) de máquinas en la telemetría de Cyber Crucible generaba alertas por comportamientos agresivos de inyección de procesos en procesos del sistema.
- Mayor capacidad de monitoreo de procesos del sistema sin firmar.
  - Esto fue en parte una respuesta a que los atacantes se enfocan intensamente en involucrar esos procesos durante operaciones de movimiento lateral (dentro de un sistema y entre sistemas).

Correcciones

- Se modificó un comportamiento de modificación de archivos para reducir los falsos positivos, dejando de activarse ante ciertas acciones benignas, mediante contexto adicional a nivel de kernel sobre los comportamientos de acceso a archivos de un proceso.

Estado de validación WHCP/WHQL

Validado.

Hashes 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 01:19:52 UTC by Dennis Underwood
Updated 2026-07-24 01:19:52 UTC by Dennis Underwood