4.4.1.0

Funcionalidades

- Suporte expandido para análises de injeção de processos, para aumentar drasticamente a precisão na deteção de intenção maliciosa versus benigna em aplicações.
  - Isto tornou-se especialmente importante devido a um pequeno número (<0.02%) de máquinas na telemetria da Cyber Crucible a alertar sobre comportamentos agressivos de injeção de processos em processos do sistema.
- Aumento da capacidade de monitorização de processos do sistema não assinados.
  - Isto foi, em parte, uma resposta ao facto de os atacantes se focarem fortemente em envolver esses processos durante operações de movimento lateral (num sistema e entre sistemas).

Correções

- Alterado um comportamento de modificação de ficheiros para diminuir os falsos positivos, deixando de ser acionado em certas ações benignas, através de contexto adicional ao nível do kernel sobre os comportamentos de acesso a ficheiros de um processo.

Estado de Validação 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 05:18:02 UTC by Dennis Underwood
Updated 2026-07-24 05:18:02 UTC by Dennis Underwood