4.4.1.3

Funcionalidades

- O Monitoramento de Credenciais/Identidade agora inclui várias VPNs, carteiras de criptomoedas e outras aplicações.
- Numa (isto é comum) cadeia de processos afetados durante um ataque (o atacante move-se do programa em execução A, para B, para C, e D é utilizado para o roubo de dados), o programa “paciente 0” A é suspenso, mas o paciente D é reportado como o processo que executa o comportamento de roubo.
  - O estado da memória é preservado e reportado ao longo de todas as cadeias de processos, para futura análise forense.
- No caso de uma resposta automatizada em que a memória de um processo em execução tenha sido modificada, essa modificação de memória é enviada de forma configurável para a Cyber Crucible para engenharia reversa e análise adicional.
- No caso de um erro de modificação de memória não malicioso numa aplicação, as exceções comportamentais (“listas de permissão”) agora têm a capacidade de sinalizar determinados eventos de corrupção de memória como benignos. Isto não impedirá que o próprio programa falhe ou perca dados devido ao erro, mas a Cyber Crucible saberá ignorar o erro ao procurar por injeção maliciosa de código em processos em execução (injeção de processo/hollowing).

Correções

- Removida vulnerabilidade em que binários podiam ser eliminados por um processo privilegiado enquanto os binários da CC estavam a ser atualizados.
- Removida vulnerabilidade em que chaves de registo podiam ser eliminadas ou alteradas por um processo privilegiado enquanto os binários da CC estavam a ser atualizados.
- Corrigido o rastreamento do estado da memória quando um processo é corrigido (patched) em memória durante a avaliação da memória pela Cyber Crucible.
- Corrigido o rastreamento do estado da memória sob determinadas condições em que a memória é realocada entre páginas de memória.
- Atualizações menores de eficiência de CPU, provavelmente demasiado pequenas para serem registadas no Gestor de Tarefas, uma vez que a utilização é normalmente <1%

Estado de Validação WHCP/WHQL

Validado

Hashes MD5

```
service.exe   = 90a6ca2f5b7a76b847052f3d420f0c9b
assistant.exe = b62ee623f74171f4a3f34ff129188174
CCRRSecMon.sys (Windows10)       = dfdce4016f6920e844615b3d506ec2e2
CCRRSecMon.sys (Windows8)        = 59bbd41c883ca0205fd3adbfdbb5dbb6
CCRRSecMon.sys (Windows7)        = 88e6f047f7fa26e717a24f5fd7b33dc5
```

4.4.1.3.1

Obtida visibilidade sobre alguns processos do sistema que se inicializam antes de o driver da Cyber Crucible ser carregado.

Hashes MD5:

```
service.exe: a03b91df83f86ffe322f7b16960f503c
assistant.exe: e22641924d3a1811b86a0f4357f74720
win7/CCRRSecMon.sys: b64b63c04f00afd1020a7a43fc0bb67d
win8/CCRRSecMon.sys: c50aacb4aac6ac9f1e95e4ffa749cb2a
win10/CCRRSecMon.sys: 77dd029b8e4b2cf5a2354787402ecc17
```

4.4.1.3.2

Adicionada telemetria adicional para os processos do sistema agora visíveis devido à versão 4.4.1.3.1.

Hashes MD5:

```
service.exe: 47f408d6102eb06a94f2244cf139a0a5
assistant.exe: 86733da51ee703f93dcda9346231cca6
win7/CCRRSecMon.sys: b01e8933fa9ac9f0a049527b20d9f679
win8/CCRRSecMon.sys: 4467124cf7e8b5ab5652169f9eb41663
win10/CCRRSecMon.sys: 8f06de95303eeac038002ec27c297811
```

4.4.1.3.3

Corrigidos alguns relatórios de incidentes que incluíam dados do processo errado, quando um processo termina a meio de um cálculo.

Hashes MD5:

```
service.exe: f2a341ca4856ab3f8a15b7cf725cd0cc
assistant.exe: 5d5d2213e276bc066f4d42ab751c7317
win7/CCRRSecMon.sys: 13da73b66751d12f5f3e65cde0602266
win8/CCRRSecMon.sys: 08fe8cb3391c9215bc37a997ec59b0a2
win10/CCRRSecMon.sys: 4c8a1707839f0d28c386f17ce2dbc8ed
```

4.4.1.3.4

Otimização dos cálculos de memória, em preparação para a versão 4.4.1.4.

Hashes MD5:

```
service.exe   = 4a5bd9822ea28c10f399afe437837a2a
assistant.exe = 7070e61862bc2ede3205c4bfdc6805d2
CCRRSecMon.sys (Windows10)       = 4e9b790522fe61e9206140e15e37b7fe
CCRRSecMon.sys (Windows8)        = 7b477503840f882028ff8bdbbfc72121
CCRRSecMon.sys (Windows7)        = 65e95b4dd58cb1c9a5dab398155e2113
```

Revision #1
Created 2026-07-24 05:18:45 UTC by Dennis Underwood
Updated 2026-07-24 05:18:45 UTC by Dennis Underwood