4.4.1.3

Funciones

- El monitoreo de credenciales/identidad ahora incluye varias VPN, billeteras de criptomonedas y otras aplicaciones.
- En una cadena (esto es común) de procesos afectados durante un ataque (el atacante se mueve del programa en ejecución A, a B, a C, y D se utiliza para el robo de datos), el programa "paciente 0" A queda suspendido, pero el paciente D se reporta como el proceso que realiza el comportamiento de robo.
  - El estado de la memoria se preserva y se reporta a lo largo de las cadenas de procesos, para un futuro análisis forense.
- En caso de una respuesta automatizada en la que se haya modificado la memoria de un proceso en ejecución, dicha modificación de memoria se sube de forma configurable a Cyber Crucible para su ingeniería inversa y análisis adicional.
- En caso de un error de modificación de memoria no malicioso en una aplicación, las excepciones de comportamiento ("listas blancas") ahora tienen la capacidad de marcar ciertos eventos de corrupción de memoria como benignos. Esto no evitará que el propio programa se bloquee o pierda datos debido al error, pero Cyber Crucible sabrá ignorar el error mientras busca la inyección maliciosa de código en procesos en ejecución (inyección de procesos/hollowing).

Correcciones

- Se eliminó una vulnerabilidad por la cual los binarios podían ser eliminados por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se eliminó una vulnerabilidad por la cual las claves de registro podían ser eliminadas o alteradas por un proceso con privilegios mientras los binarios de CC se estaban actualizando.
- Se corrigió el seguimiento del estado de la memoria cuando un proceso se parchea en memoria durante la evaluación de la memoria por parte de Cyber Crucible.
- Se corrigió el seguimiento del estado de la memoria en determinadas condiciones en las que la memoria se reasigna entre páginas de memoria.
- Actualizaciones menores de eficiencia de la CPU, probablemente demasiado pequeñas para registrarse en el Administrador de tareas, ya que el uso normalmente es <1%

Estado de validación 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

Se obtuvo visibilidad sobre algunos procesos del sistema que se inicializan antes de que se cargue el controlador de Cyber Crucible.

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

Se agregó telemetría adicional para los procesos del sistema ahora visibles debido a 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

Se corrigieron algunos reportes de incidentes que incluían datos del proceso incorrecto, cuando un proceso finaliza a mitad de un 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

Optimización de los cálculos de memoria, en preparación para la 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 01:20:38 UTC by Dennis Underwood
Updated 2026-07-24 01:20:38 UTC by Dennis Underwood