4.4.5.2

Características

- Nueva telemetría de acceso a nivel de kernel para comportamientos basados en red, con el fin de identificar mejor posibles errores de red del lado del cliente, u oportunidades de optimización
- La telemetría saliente ahora se agrupa y se envía en conjunto, al igual que la configuración entrante
  - Transmitida con una variación de tiempo del 25%, para que no todas las máquinas envíen paquetes simultáneamente a través de una red de clientes
- HTTP/2 ahora se utiliza completamente de extremo a extremo

Correcciones

- Se redujo el número mínimo de subprocesos en uso en el espacio de usuario
- Se redujo el uso de CPU para el servicio de espacio de usuario
- La autenticación Agente-Servidor ahora se realiza de manera más eficiente
- Se reemplazó el algoritmo anterior de suspensión <> reinicio del servicio cuando las licencias no estaban disponibles.
  - El algoritmo anterior causaba un "el servicio finalizó inesperadamente" en el administrador de eventos cada 15 minutos.
  - Permitir que el sistema operativo indique al servicio que se apague (algo que ha sido explotado por delincuentes y otras herramientas de seguridad) habría permitido un reinicio "limpio" del servicio sin registros en el administrador de eventos. En lugar de crear esa vulnerabilidad, el servicio de Cyber Crucible se reinició por sí mismo sin la intervención de Windows, provocando el registro de eventos.

Hashes MD5

```
service.exe  = b17a2a528a4424771fdeca8559b9f56b
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Revision #1
Created 2026-07-24 01:23:07 UTC by Dennis Underwood

Updated 2026-07-24 01:23:07 UTC by Dennis Underwood