

4.5.3.2

Características

- FortressAI
 - Ninguna
- Cyber Crucible Core
 - Mejora de la operación del búfer del kernel
 - El controlador utiliza búferes para almacenar temporalmente la telemetría que finalmente se envía al panel del cliente. Esta actividad es distinta de la población o las operaciones del modelo de comportamiento.
 - Si un búfer del kernel se sobrecarga, la carga de CPU del sistema aumenta.
 - Esto solo ocurriría debido a un gran error del sistema operativo o a un ataque a los sistemas.
 - La notificación automática al cliente sobre un uso de búfer muy alto estará disponible el 1 de junio de 2026.
 - Casi todas las operaciones del búfer del kernel de CC corresponden a tres búferes principales.
 - El porcentaje de uso de los tres búferes principales ahora se transmite a la infraestructura de CC para la recopilación de métricas y la identificación del uso de búfer por agente.
 - Los tres búferes principales pueden ajustarse en tamaño de forma remota, y los usuarios pueden hacer seguimiento de su estado.

Correcciones

- Una actualización reciente relacionada con las bibliotecas redistribuibles de DotNet y MSVC saturó los búferes de Cyber Crucible con eventos sostenidos y muy altos (500%+) de operaciones de procesos y DLL, lo que afectó a algunos clientes. Aunque el uso del búfer ha vuelto al nivel normal del 1-5%, incluidos los clientes afectados, se duplicó el tamaño de todos los búferes para prevenir posibles problemas futuros. Esto se suma a las capacidades de configuración mencionadas anteriormente.

Hashes Sha-256

```
service.exe = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
CCRRSecMon.sys = d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
CCRRSecMon.inf = db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat = a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486
```

Revision #1

Created 2026-07-24 01:28:57 UTC by Dennis Underwood

Updated 2026-07-24 01:28:57 UTC by Dennis Underwood