4.5.3.2

Features

- FortressAI
  - None
- Cyber Crucible Core
  - Kernel Buffer Operation Enhancement
    - The driver leverages buffers to temporarily store telemetry that is ultimately sent to the customer dashboard. This activity is distinct from behavioral model population or operations.
    - If a kernel buffer overloads, system CPU load increases.
      - This would only happen due to a large OS bug or an attack on the systems.
      - Automated customer notification of very high buffer usage available 1 JUN 2026.
    - Almost all of the kernel buffer operations for CC are with three primary buffers.
    - All three primary buffers' usage percentage is now transmitted to the CC infrastructure for metrics gathering and identification of buffer usage on a per-agent basis.
    - All three primary buffers are able to be adjusted in size remotely, and their status tracked by users.

Fixes

- A recent update involving DotNet and MSVC Redistributable libraries overwhelmed Cyber Crucible buffers with sustained very high (500%+) process and DLL operations events, affecting some customers. Though buffer usage is back down to the normal 1-5% usage, including the impacted customers, all buffers were doubled in size to account for any future issues. This is in addition to the configuration capabilities listed above.

Sha-256 Hashes

```
service.exe  = 2f46657af8809339d16546f1e6f2b58975bbf4d5c10fde3510363d628b129492
fai-alert.exe  = 890ccca7e0ce14a0e2ff7f90bae75a7ef12ad6c8cd43ffb52093c8431e65770b
CCRRSecMon.sys   = d0e941bc25d31e38cbebbe9ce3918f82d0b9c7b433efed318cb34e36a50acf94
```

```
CCRRSecMon.inf   = db54d8077afdfef81286868f7bda1e8df17dbd812178ddac989127550a904a8c
ccrrsecmon.cat   = a01c31db7231fed3852c9e559eb2c3f7496a016982207c102b88d8b36dcb0486
```

Revision #1
Created 2026-07-13 18:50:22 UTC by Dennis Underwood
Updated 2026-07-13 18:50:22 UTC by Dennis Underwood