4.4.5.2

Features

- New kernel level access telemetry for network-based behaviors, to better identify possible client-side networking bugs, or opportunities to optimize
- Outbound telemetry is now bundled and sent together, just like inbound settings
  - Transmitted with a 25% timing variance, so that every machine will not be sending packets simultaneously across a client network
- HTTP/2 is now fully utilized end to end

Fixes

- Reduced minimum threads in use in userspace
- Reduced CPU usage for userspace service
- Agent-Server authentication is now performed more efficiently
- Replaced previous service sleep <> restart algorithm when licenses were not available.
  - Previous algorithm caused a "service exited unexpectedly" in event manager every 15 minutes.
  - Allowing the Operating System to tell the service to shut off (something abused by criminals and other security tools) would have allowed a “clean” service restart without event manager logs. Instead of creating that vulnerability, Cyber Crucible’s service restarted itself without Windows involvement, causing the event log.

MD5 Hashes

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

Revision #1
Created 2026-07-13 18:49:38 UTC by Dennis Underwood
Updated 2026-07-13 18:49:38 UTC by Dennis Underwood