4.4.5.2

Funktionen

- Neue Telemetrie auf Kernel-Ebene für netzwerkbasierte Verhaltensweisen, um mögliche clientseitige Netzwerkfehler besser zu identifizieren oder Optimierungsmöglichkeiten zu erkennen
- Ausgehende Telemetrie wird nun gebündelt und gemeinsam gesendet, genau wie die eingehenden Einstellungen
  - Übertragung mit einer zeitlichen Abweichung von 25 %, sodass nicht alle Geräte gleichzeitig Pakete über ein Client-Netzwerk senden
- HTTP/2 wird nun durchgängig vollständig genutzt

Fehlerbehebungen

- Reduzierte minimale Anzahl an genutzten Threads im Userspace
- Reduzierte CPU-Auslastung für den Userspace-Dienst
- Die Authentifizierung zwischen Agent und Server wird nun effizienter durchgeführt
- Der bisherige Algorithmus für Dienst-Ruhezustand <> Neustart wurde ersetzt, wenn keine Lizenzen verfügbar waren.
  - Der bisherige Algorithmus verursachte alle 15 Minuten einen Eintrag „Dienst wurde unerwartet beendet“ im Ereignis-Manager.
  - Es dem Betriebssystem zu erlauben, den Dienst abzuschalten (was von Kriminellen und anderen Sicherheitstools missbraucht wird), hätte einen „sauberen“ Dienst-Neustart ohne Einträge im Ereignis-Manager ermöglicht. Anstatt diese Schwachstelle zu schaffen, startete sich der Dienst von Cyber Crucible selbst neu, ohne Einbindung von Windows, was zu dem Ereigniseintrag führte.

MD5-Hashes

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

Revision #1
Created 2026-07-24 04:05:13 UTC by Dennis Underwood

Updated 2026-07-24 04:05:13 UTC by Dennis Underwood