

4.4.1.0

Funktionen

- Erweiterte Unterstützung für Analysen von Prozessinjektionen, um die Genauigkeit der Erkennung von böswilliger vs. gutartiger Absicht bei Anwendungen erheblich zu steigern.
 - Dies wurde besonders wichtig, da eine geringe Anzahl (<0,02 %) der Maschinen in der Cyber-Crucible-Telemetrie Warnungen zu aggressivem Prozessinjektionsverhalten von Systemprozessen auslöste.
- Verbesserte Überwachungsfähigkeit für unsigned Systemprozesse.
 - Dies war teilweise eine Reaktion darauf, dass Angreifer sich stark darauf konzentrieren, diese Prozesse bei seitlichen Bewegungsoperationen (innerhalb eines Systems und zwischen Systemen) einzubeziehen.

Fehlerbehebungen

- Ein Verhalten bei Dateiänderungen wurde geändert, um Fehlalarme zu reduzieren, indem bestimmte gutartige Aktionen nicht mehr ausgelöst werden – durch zusätzlichen Kernel-Level-Kontext zu den Dateizugriffsverhaltensweisen eines Prozesses.

WHCP/WHQL-Validierungsstatus

Validiert.

MD5-Hashes

```
service.exe      = 0bab8404900c6a16ac3ad0293c45de5c
assistant.exe    = 98f013fd4fdb7325f903d07c87b999ac
CCRRSecMon.sys (Windows10)      = 452719399d9bb98dc6b14fb8787d8415
CCRRSecMon.sys (Windows8)       = a974c7cc46db3759a2da34f37caaa72e
CCRRSecMon.sys (Windows7)       = 6a0f2e55d6a7b66bd9bbe318d5dbbebf
```

Revision #1

Created 2026-07-24 04:01:52 UTC by Dennis Underwood

Updated 2026-07-24 04:01:52 UTC by Dennis Underwood