

4.4.8.1

Funktionen

- Ausführbare Metadaten wie Produktversion, Firmenname usw. für Prozesse im Arbeitsspeicher werden vom Treiber über Kernel-Sichtbarkeit gemeldet. Normale Funktionalität ist die Verwendung von Windows-API-Aufrufen im User-Space. Diese Umstellung auf das Parsen im Kernel entfernt die (beobachtete) Möglichkeit für Angreifer, die Prozessinformationen zu manipulieren.
- Authentifizierungsinformationen des Agenten werden an anderer Stelle im System repliziert, um sie wiederherzustellen, falls die Registrierung durch einen bösartigen Treiber beschädigt wird.

Verbesserungen

- Serververbindungsfehler werden vom Agenten nur minimal protokolliert, wodurch die Protokollgröße auf der Festplatte reduziert wird.

Fehlerbehebungen

- Entfällt

MD5-Hashes

```
service.exe = 8c1f6999ccd176193e493686216f14c6
CCRRSecMon.sys (Windows7) = 3b032d0e43674509126c6cb1c9efd688
CCRRSecMon.sys (Windows8) = d3131131c83c2cf833ebc2157149c364
CCRRSecMon.sys (Windows10) = eac8a8b38a8743a13dd7130509de9907
```

Revision #1

Created 2026-07-24 04:08:36 UTC by Dennis Underwood

Updated 2026-07-24 04:08:37 UTC by Dennis Underwood