

4.4.8.1

Features

- Executable metadata such as product version, company name, etc. for in-memory processes are reported by the driver via kernel visibility. Normal functionality is to use user-space Windows API calls. This move to parsing in the kernel removing the (observed) opportunity for attackers to tamper with the process information.
- Agent authentication information is replicated elsewhere in the system to restore in the event the registry is corrupted by a malicious driver.

Enhancements

- Server connection errors are minimally logged by the agent, reducing log size on disk.

Fixes

- N/A

MD5 Hashes

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

Revision #1

Created 2026-07-13 18:50:00 UTC by Dennis Underwood

Updated 2026-07-13 18:50:00 UTC by Dennis Underwood