

4.4.5.9

Features

- Increased hardening of portions of functionality previously conducted by the Windows cryptography libraries are done conducted by the Cyber Crucible kernel driver.
 - This is both general hardening, and an increase in telemetry indicating possible attacks against Windows cryptography libraries and APIs.
- This is a milestone release from incremental releases found in 4.4.5.4 - 4.4.5.8, all aligned on the previous cryptography analysis hardening functionality.
 - Early telemetry indicates the failures in Windows certificate and cryptography libraries were legitimately responded to by Cyber Crucible.
 - It is unknown at this time what percentage of issues were due to exploitation vs a Windows core library bug. Please contact your Cyber Crucible representative to discuss further as necessary.

Fixes

- Fixed some process reports incorrectly reporting the listed certificate as “not trusted”, due to Windows certificate library functionality loss.

MD5 Hashes

```
service.exe = 79650eea0a93b8f480b4247d57ddd03b
CCRRSecMon.sys (Windows7) = 06a647c897f9f385416482a4e899e204
CCRRSecMon.sys (Windows8) = 72c1b462e3e8e3fa4dcf6344ce3b0acd
CCRRSecMon.sys (Windows10) = 02b1c53268059ae38427fe43152d593c
```

Revision #1

Created 2026-07-13 18:49:42 UTC by Dennis Underwood

Updated 2026-07-13 18:49:42 UTC by Dennis Underwood