

4.4.8.1

Características

- Los metadatos ejecutables, como la versión del producto, el nombre de la empresa, etc., para los procesos en memoria son informados por el controlador mediante visibilidad a nivel de kernel. La funcionalidad normal es utilizar llamadas a la API de Windows en espacio de usuario. Este cambio hacia el análisis en el kernel elimina la oportunidad (observada) de que los atacantes manipulen la información del proceso.
- La información de autenticación del agente se replica en otra parte del sistema para poder restaurarla en caso de que el registro sea corrompido por un controlador malicioso.

Mejoras

- Los errores de conexión al servidor son registrados de forma mínima por el agente, reduciendo el tamaño del registro en disco.

Correcciones

- N/A

Hashes MD5

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

Revision #1

Created 2026-07-24 01:26:06 UTC by Dennis Underwood

Updated 2026-07-24 01:26:06 UTC by Dennis Underwood