4.4.5.2

Recursos

- Nova telemetria de acesso em nível de kernel para comportamentos baseados em rede, para melhor identificar possíveis bugs de rede no lado do cliente, ou oportunidades de otimização
- A telemetria de saída agora é agrupada e enviada em conjunto, assim como as configurações de entrada
  - Transmitida com uma variação de tempo de 25%, para que nem todas as máquinas enviem pacotes simultaneamente em uma rede de clientes
- O HTTP/2 agora é totalmente utilizado de ponta a ponta

Correções

- Redução do número mínimo de threads em uso no espaço do usuário
- Redução do uso de CPU pelo serviço em espaço do usuário
- A autenticação Agente-Servidor agora é realizada de forma mais eficiente
- Substituído o algoritmo anterior de suspensão/reinício do serviço quando as licenças não estavam disponíveis.
  - O algoritmo anterior causava um "serviço encerrado inesperadamente" no gerenciador de eventos a cada 15 minutos.
  - Permitir que o Sistema Operacional instrua o serviço a desligar (algo explorado indevidamente por criminosos e outras ferramentas de segurança) teria permitido um reinício "limpo" do serviço sem registros no gerenciador de eventos. Em vez de criar essa vulnerabilidade, o serviço da Cyber Crucible se reiniciou sozinho sem o envolvimento do Windows, gerando o registro de evento.

Hashes MD5

```
service.exe  = b17a2a528a4424771fdeca8559b9f56b
CCRRSecMon.sys (Windows7)        = c2b051b1001474419e7572fd23625d84
CCRRSecMon.sys (Windows8)        = 335d355bbd492c390e67ac615c5252b0
CCRRSecMon.sys (Windows10)       = 0d1fc32fba2cb878ce8cb0f549b8d167
```

Revision #1
Created 2026-07-24 05:21:08 UTC by Dennis Underwood

Updated 2026-07-24 05:21:08 UTC by Dennis Underwood