Falhas críticas são encontradas em app open-source de criptografia

Uma nova auditoria de segurança encontrou vulnerabilidades críticas no VeraCrypt, um programa open-source de criptografia completa que é o sucessor direto do muito popular e agora morto TrueCrypt.

Os usuários são encorajados a fazer um upgrade para o VeraCrypt 1.19, que foi liberado nesta semana e inclui patches para a maioria das falhas. Alguns problemas continuam sem solução porque corrigi-los exige mudanças complexas no código e em alguns casos afetaria a compatibilidade reversa com o TrueCrypt.

No entanto, o impacto da maioria desses problemas podem ser evitados ao seguir as práticas seguras mencionadas na documentação ao configurar contêineres criptografados e usando o software.

A auditoria, que foi realizada pela empresa francesa de segurança Quarkslab e patrocinada pelo Open Source Technology Improvement Fund (OSTIF), encontrou oito vulnerabilidades críticas, três de risco médico e 15 falhas de baixo impacto. Algumas delas são problemas sem patches descobertos anteriormente em uma auditoria anterior da TrueCrypt.

Muitas falhas estavam localizadas no bootloader do VeraCrypt para computadores e sistemas que usam a nova UEFI (Unified Extensible Firmware Interface) – a BIOS moderna. O TrueCrypt, que serve como base para o VeraCrypt, nunca teve suporte para a UEFI, forçando os usuários a desabilitar o BOOT da UEFI caso queiram criptografar a partição do sistema.

O bootloader do VeraCrypt compatível com UEFI – o primeiro

para programas open-source de criptografia no Windows – foi lançado em agosto e é maior adição ao código base do TrueCrypt feita pelo desenvolvedor chefe do VeraCrypt, Mounir Idrassi. Isso o torna muito menos maduro do que o restante do código, por isso é compreensível que possa ter mais falhas.

Outra mudança feita após a auditoria foi a remoção do padrão de criptografia Russian GOST 28147-89, cuja implementação foi classificada como insegura pelos auditores.

Fonte: http://idgnow.com.br/internet/2016/10/18/falhas-criticas-sao-encontradas-em-app-open-source-de-criptografia/