Alerta de Segurança 001/2020 –Cogetic/VPGDI

Em 16 de janeiro de 2020

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidade CVE-2020-0601

Prezados Gestores de TI da Fiocruz, encaminhamos Alerta de Segurança sobre vulnerabilidade Sistema Operacional Windows.

Descrição do problema

A *National Security Agency* – NSA informa que que a vulnerabilidade CVE-2020-0601 permite que seja realizada uma falsificação na maneira como o Windows CryptoAPI (Crypt32.dll) valida certificados ECC (*Elliptic Curve Cryptography*).

Esta vulnerabilidade afeta os sistemas operacionais Windows 10, incluindo versões de servidor (Windows Server 2016 e Windows Server 2019).

Descrição dos ataques

Um invasor pode explorar a vulnerabilidade usando um certificado de assinatura de código falsificado para assinar um executável malicioso, fazendo parecer que o arquivo era de uma fonte confiável e legítima, também conhecida como 'Vulnerabilidade de falsificação do Windows CryptoAPI'.

Uma exploração bem-sucedida também pode permitir que o invasor realize ataques *man-in-the-middle* e descriptografe informações confidenciais sobre as conexões dos usuários com o software afetado.

Recomendações

Verificar e instalar as atualizações de segurança disponíveis mais recentes para os sistemas operacionais afetados Windows 10, Windows Server 2016 e Windows Server 2019:

Referências

- https://msrc-blog.microsoft.com/2020/01/14/january-2020-security-updates-cve-2020-0601/
- https://research.kudelskisecurity.com/2020/01/15/cve-2020-0601-the-chainoffools-attack-explained-with-poc/amp/?__twitter_impression=true
- https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2056772/a-very-important-patch-tuesday/

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações