Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 004/2020 - Cogetic

Em 16 de setembro de 2020

Para: Gestores de TI das unidades da Fiocruz

Assunto: CVE-2020-1472 - Vulnerabilidade Zerologon

Prezados Gestores de TI,

A vulnerabilidade CVE-2020-1472 se aproveita de falha no modelo de autenticação criptográfica do protocolo remoto Netlogon (MS-NRPC) em sistemas operacionais Windows. O Netlogon é um compartilhamento de rede localizado em controladores de domínios de rede, contendo scripts para logon de usuários e de computadores.

Um atacante não autenticado pode se aproveitar dessa falha para estabelecer uma conexão segura com um Domain Controller, por meio de Netlogon vulnerável, conquistando elevação de privilégio não autorizado.

A Microsoft disponibilizou em agosto de 2020 correções de segurança para esta vulnerabilidade. Mais recentemente foram disponibilizados na Internet *exploits* dessa vulnerabilidade, aumentando potencialmente o seu risco de exploração. Assim, recomendamos a atualização do sistema operacional de forma imediata, conforme orientações da fabricante Microsoft.

Recomendamos que os controladores de domínio Windows estejam com o agente do Deep Security instalado, com o módulo de IPS habilitado, com *Prevent Mode* ativado, e com a regra de "Microsoft Windows Netlogon Elevation Of Privilege Vulnerability (CVE-2020-1472)" corretamente assinada.

Ressaltamos, contudo, que a funcionalidade de *Virtual Patching* do Deep Security não é uma solução de gestão de patchs, sendo importante a atualização da aplicação com a patch disponibilizado pelo fabricante o quanto antes.

Referências:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

- https://olhardigital.com.br/noticia/vulnerabilidade-grave-do-windows-permite-invasao-do-computador/107041
- https://www.kaspersky.com/blog/cve-2020-1472-domain-controller-vulnerability/37048/
- https://nvd.nist.gov/vuln/detail/CVE-2020-1472

Coordenação-Geral de Gestão de Tecnologia da Informação
Serviço de Segurança da Informação e Comunicações