Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 005/2019 - Cogetic

Em 9 de setembro de 2019

Para: Gestores de TI das unidades da Fiocruz

Assunto: BlueKeep

Prezados Gestores de TI,

A execução remota de códigos é uma vulnerabilidade presente nos Serviços de Área de Trabalho Remota, anteriormente conhecidos como Serviços de Terminal, que permite a um invasor não autenticado se conectar ao sistema de destino usando RDP e executar remotamente códigos maliciosos.

A vulnerabilidade está descrita na CVE-2019-0708, também conhecida como BlueKeep, estando presente em versões do sistema operacional Windows sem suporte pelo fabricante (Windows XP, Windows 2003, Windows 7, Windows Server 2008 e Windows Server 2008 R2).

Para as unidades instaladas no *campus* da Fiocruz em Manguinhos, foi aplicada a assinatura MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution no serviço IPS. Orientamos que as demais unidades com solução própria de IPS ativem assinatura equivalente.

Outra medida importante é a ativação da regra 1009749 [Microsoft Windows Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)] no módulo IPS do Deep Security. Observem que as regras de IPS, por padrão, estão no modo de detecção. Assim, faz-se necessário ativar o modo de prevenção para que se tenha proteção efetiva.

Por fim, recomendamos a instalação da atualização disponibilizada pela Microsoft para as plataformas XP, Server 2003 e Vista, dado o potencial impacto para esses sistemas operacionais. As atualizações estão disponíveis em https://support.microsoft.com/pt-br/help/4500705/customer-guidance-for-cve-2019-0708

Embora a CVE-2019-0708 não seja novidade, no ultimo dia 6 de setembro de 2019, a Rapid7 publicou um *Metasploit* para o *BlueKeep*, obtendo sucesso na exploração da falha. Há relatos de intensas atividades de exploração da vulnerabilidade na Internet e já detectamos atividades na rede da Fiocruz, todas elas contidas pelo IPS.

Em caso de dúvidas sobre a configuração da política do Deep Security ou qualquer outro esclarecimento sobre este evento, favor abrir uma RSI no serviço “Deep Security” e na opção “Apoio para configuração de política”.

Referências:

— https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

— https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/metasploit-team-releases-bluekeep-exploit/

— https://fortiguard.com/encyclopedia/ips/47968

— https://support.microsoft.com/pt-br/help/4500705/customer-guidance-for-cve-2019-0708

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações