



Ministério da Saúde

FIOCRUZ

Fundação Oswaldo Cruz

Alerta de Segurança 001/2021 - Cogetic

Em 10 de fevereiro de 2021

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidade em SO Windows [CVE-2021-1732]

Prezados Gestores de TI,

Foi identificada uma vulnerabilidade no driver Win32k que permite escalção de privilégios e habilita um invasor local a assumir o controle de administrador do sistema operacional. Já foram identificados *exploits* disponíveis publicamente para esta falha, aumentando exponencialmente o risco de exploração.

Recomendação

Recomendamos aos administradores de servidores com Sistemas Operacionais Windows 10 e Windows 2019 consultar o link abaixo e aplicar o patch correspondente com URGÊNCIA.

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1732>

Referências

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1732>

<https://news.sophos.com/en-us/2021/02/09/frag-out-four-remote-attack-bugs-fixed-in-microsofts-february-patch-tuesday/>

<https://threatpost.com/exploited-windows-kernel-bug-takeover/163800/>

<https://vuldb.com/?id.169518>

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