

Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 004/2019 - Cogetic

Em 6 de maio de 2019

Para: Gestores de TI das unidades da Fiocruz

Assunto: Atualização de sistema operacional

Prezados Gestores de TI,

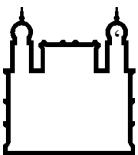
Manter o sistema operacional atualizado, bem como serviços e aplicações, é uma boa prática de segurança e traz uma série de benefícios, tais como correção de falhas, introdução de novos recursos, melhora de desempenho, entre outros. Muitos softwares para funcionar de efetiva, necessitam utilizar os recursos disponíveis nas versões mais recentes do sistema operacional.

Ter um sistema operacional atualizado é um pré-requisito para o adequado funcionamento da solução Trend Micro Deep Security. A versão disponível do agente será compatível apenas com versões recentes e atualizadas dos sistemas operacionais. Versões antigas e desatualizadas, embora permitam a instalação do agente, impedem o funcionamento das funcionalidades da solução de segurança.

Embora seja possível fazer o *downgrade* da versão do agente do Deep Security para permitir a instalação em sistemas operacionais desatualizados, essa prática traz dois efeitos colaterais:

- 1) Não utilização de todos os recursos da versão mais atual do Deep Security;
- 2) Caso haja uma atualização do Deep Security, o agente (com *downgrade*) se tornará obsoleto, deixando o host desprotegido.

Hoje, observa-se uma grande quantidade sistemas operacionais desatualizados, como RedHat 5, Ubuntu 14, entre outros. Isso apresenta um duplo riscos, pois existem vulnerabilidades já corrigidas pelo fabricante que não estão instaladas e a impossibilidade de proteção pelo Deep Security.



Ministério da Saúde

FIOCRUZ

Fundaçao Oswaldo Cruz

Assim, recomenda-se que se mantenham os servidores sempre atualizados, para que eles tenham compatibilidade com o agente do Deep Security e estejam protegidos contra novas vulnerabilidades e ameaças e utilizando toda a potencialidade da solução de segurança.

Referências:

- <https://help.deepsecurity.trendmicro.com/software-feature-releases.html>

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações