AVISO DE PRODUTO

Assunto:	***Medidas de proteção contra ransomware/malware Sistemas TrueBeam™, VitalBeam™ de radioterapia e EDGE™ Radiosurgery***
Referência:	**CP-30654**
Data da notificação:	***07/08/2017***
Tipo de ação:	**Notificação – Comunicado**

DESCRIÇÃO DO PROBLEMA:

Recentemente, foram noticiados diversos ataques cibernéticos graves em provedores de saúde, incluindo os vírus WannaCry, EternalBlue e Petya/NotPetya. A Varian desenvolveu uma melhoria para impedir ransomware e outros tipos de ataques de malware em computadores nos quais produtos de software da Varian® estão instalados.

DETALHES:

Um malware é qualquer tipo de software projetado com a intenção de causar danos ou desabilitar computadores e sistemas de informática. Um ransomware é um tipo específico de malware que impede as empresas de usarem estações de trabalho, servidores, arquivos e redes, fazendo deles reféns até o pagamento de um resgate. A Varian recebeu duas denúncias de invasões de software em Sistemas de aplicação de tratamento de radiação TrueBeam® especificamente relacionados a explorações do ransomware WannaCry. O WannaCry, o EternalBlue e o Petya/NotPetya exploram a vulnerabilidade do protocolo de transferência de dados de SMB. Esses vírus ransomware invadem, criptografam dados e exibem um banner com o pedido de resgate para que os dados sejam descriptografados. Em seguida, esse ransomware pode se propagar pela rede para outros dispositivos.

A melhoria de produto da Varian atualizará o Dispositivo de Interface de Rede do Cliente (CNID, também conhecido como MICAP) e eliminará essa vulnerabilidade no ponto de acesso de transferência de dados de SMB. O fluxo de trabalho clínico não será afetado pela implementação dessa melhoria de produto.

AÇÃO RECOMENDADA AO USUÁRIO:

1) Leia e preencha o formulário em anexo para ***aceitar*** a implantação remota automática da Varian da melhoria de produto em questão. Envie o formulário para a Varian assim que possível: returnresponse@varian.com.
2) Entre em contato com seu representante de serviço da Varian para ***recusar*** a implantação remota automática da Varian da melhoria de produto em questão.
3) Entre em contato com seu representante de serviço da Varian para discutir quaisquer dúvidas sobre a implantação remota automática da Varian da melhoria de produto em questão.

AÇÃO RECOMENDADA AO USUÁRIO: se você for infectado por um ransomware

1) Desconecte o computador afetado da rede e da Internet imediatamente.
2) Notifique o setor de TI local sobre a invasão.
3) Entre em contato com o representante de serviços da Varian Medical Systems para obter ajuda para restaurar os dados criptografados pelo ransomware.

AÇÃO DA VARIAN:

1) A Varian implantará o aprimoramento do produto por atualização AutoRemote da seguinte forma:
    a. AMÉRICAS – 8 de setembro de 2017
    b. EMEAI – 15 de setembro de 2017
    c. APAC – 22 de setembro de 2017