\

Nota de Segurança Urgente:

Aparelho AQT90 FLEX,
CVE-2019-0708 Protocolo de Vulnerabilidade do Remote Desktop Services (BlueKeep)

Prezado Cliente,

Em 14 de Maio de 2019 a Microsoft divulgou um patch para uma vulnerabilidade de um Código de Execução Remota crítico no Remote Desktop Services (CVE-2019-0708). Essa vulnerabilidade pode ser explorada remotamente sem autenticação nos sistemas que usam o Remote Desktop Services para os Sistemas Operacionais, Windows XP, Windows 7, Windows Server 2003 e Windows Server 2008.
A RADIOMETER utiliza os RXPE e RWES7, os quais são versões embutidas dos sistemas operacionais Windows XP e Windows 7 customizados para nossas aplicações. Essas versões possuem funcionalidades limitadas comparadas com a versão complete e por essa razão a vulnerabilidade é limitada a versão indicada no produto afetado.

A vulnerabilidade pode ser explorada no seguinte cenário:
Passo 1: Um invasor remoto conecta-se ao aparelho.
Passo 2: O invasor usa o Remote Desktop Protocol para enviar uma mensagem que pode:
- Habilitar a execução de um software malicioso e espalhar pela rede.
- Causar uma corrupção de memória no aparelho, que resultaria na "Blue Screen of Death" ou numa reinicialização do mesmo.

Proteção geral do aparelho, dados do paciente e sistema operacional
O setup do aparelho provê proteção extensiva aos seguintes sistemas:
- O Banco de Dados é encripitado e protegido por senha e demanda um alto nível de conhecimento para se roubar dados.
- A partição do Sistema (C: drive) do dispositivo é protegida contra gravações, então alterações no drive do sistema não são possíveis.

Riscos para o paciente
Num razoável e previsto pior cenário, o erro descrito pode causar uma demora na medida da pO2 num paciente crítico com hipoxemia crítica. A demora de até 10 minutos pode atrasar tratamentos importantes do paciente e colocá-lo num aumento de risco de cianose e baixa pressão sanguínea. Entretanto, o erro descrito não é considerado capaz de resultar em danos cerebrais e morte baseados em hipoxemia não diagnosticada.

Produto afetado:
AQT90 FLEX com as seguintes versões de sistema operacional:

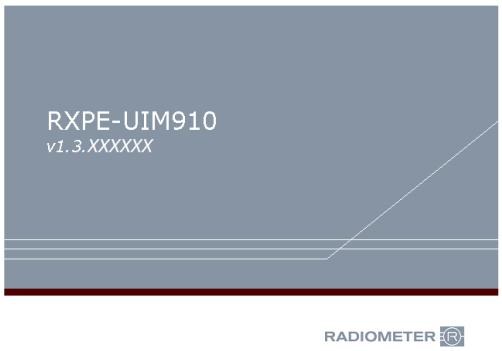
RXPE v1.3xxxxxx

(os seis dígitos após v1.3 variam e não são importantes)

Essa versão em particular, esta instalada somente nos AQT90 Flex, 393-838, com números de série abaixo de R0362N001.

O quê você deve fazer:

- Checar qual a versão de Sistema operational (OS) instalada no seu aparelho, da seguinte maneira:
  - Faça o Logon no aparelho
  - Toque *Menu*, *Utilidades*, Shutdown*Temporário e então Confirmar*
  - Durante o processo o aparelho mostra na tela a versão da OS instalada
- Se a versão do OS for uma das descritas nas figuras abaixo seu aparelho esta afetado pela vulnerabilidade:



- Se o seu aparelho estiver afetado pela vulnerabilidade, as seguintes opções terão que ser aplicadas:

  Curto prazo: Se o seu aparelho estiver conectado a rede e o seu Departamento de TI avaliar que o Firewall do Hospital e os setups da rede previnem ataques remotos de se conectarem com o aparelho e explorar a vulnerabilidade, você pode decidir manter o aparelho conectado. Caso contrário, recomendamos que o mesmo seja desconectado até que as contramedidas de logo prazo sejam implementadas.

  Longo prazo: **Contramedida 1:**
  Contate seu Representante Radiometer para instalar a atualização de segurança no RXPE no seu aparelho. (Nota: A Microsoft não dá suporte ao Windows XP. Entretanto, devido a essa vulnerabilidade lançaram esse patch de segurança).

  ou

  Contramedida 2:
  Contate seu Representante Radiometer para receber uma cotação para uma atualização para a última versão do OS da Radiometer com suporte Microsoft.

Nota:

Se você não é usuário final do produto afetado, favour assegurar-se de que esse e-mail seja distribuído para os usuários finais.
Em caso de duvidas, contate o Representante Radiometer mais próximo.

Atenciosamente,
BIODINA INSTRUMENTOS CIENTÍFICOS LTDA

Sylvio dos Santos Jr.
Responsável Técnico
E-mail: sylvio.sj@biodina.com.br