Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 08/2017 – Redução de risco de SNMP *Abuse*

1. Descrição do Problema

O protocolo SNMP habilitado e mal configurado pode sofrer abuso com a finalidade de se obter acesso não autorizado a dispositivos de rede. O SNMP fornece uma estrutura de linguagem padrão, sendo usado para monitoramento e gerenciamento de dispositivos em uma rede.

2. Possíveis Riscos

O SNMP depende de *strings* seguras que concedem acesso a porções de planos de gerenciamento de dispositivos. O abuso de SNMP pode permitir que um terceiro não autorizado obtenha acesso a um dispositivo de rede.

O SNMPv3 deve ser a única versão do SNMP empregada porque o SNMPv3 tem a capacidade de autenticar e criptografar *payloads*. Quando SNMPv1 ou SNMPv2 são empregados, um atacante pode escutar/monitorar o tráfego de rede para determinar as *strings* seguras. Esse comprometimento poderia permitir um *man-in-the-middle* ou *replay attack.*

Embora SNMPv1 e SNMPv2 tenham características semelhantes, contadores de 64 bits foram adicionados ao SNMPv2 para que ele possa suportar interfaces mais rápidas. O SNMPv3 substitui o compartilhamento de senha de texto simples/claro usado no SNMPv2 com parâmetros codificados de forma mais segura. Todas as versões são executadas sobre o *User Datagram Protocol* (UDP).

Simplesmente usar o SNMPv3 não é suficiente para evitar o abuso do protocolo. Uma abordagem mais segura é combinar SNMPv3 com *management information base* (MIB) usando SNMP *views* . Esta técnica garante que, mesmo com credenciais expostas, as informações não sejam ou escritas no dispositivo, a menos que as informações sejam necessárias para o monitoramento ou a reconfiguração normal do dispositivo. A maioria dos dispositivos que suportam SNMP contém um conjunto genérico de MIBs que são de fornecedores desconhecidos. Essa abordagem permite que o *object identifier* (OID) seja aplicado a dispositivos independentemente do fabricante.

3. Dispositivos afetados

Dispositivos habilitados para *Simple Network Management Protocol* (SNMP).

4. Sugestões para Mitigação do Problema

- Só habilite o protocolo SNMP caso seja necessário.

- Configure o SNMPv3 para usar o mais alto nível de segurança disponível no dispositivo; ele usaria autenticação *authPriv* na maioria dos dispositivos. *authPriv* inclui recursos de autenticação e criptografia, e o uso de ambos os recursos aumenta a segurança geral da rede. Algumas imagens antigas podem não conter o conjunto de recursos criptográficos, caso em que *authNoPriv* precisa ser usado. No entanto, se o dispositivo não suportar a versão 3 *authPriv*, ele deve ser atualizado;
- Certifique-se de que as credenciais administrativas estão devidamente configuradas com senhas diferentes para autenticação e criptografia. Na configuração de contas, siga o princípio do menor privilégio. A separação de funções entre as armadilhas de recepção / recepção (leitura) e a configuração de usuários ou grupos (escrita) é imperativa porque muitos gerentes SNMP requerem credenciais de *login* para serem armazenadas no disco para receber *traps*;
- Consulte o guia com orientações do seu fornecedor para implementar SNMP *views*. SNMP *views* é um comando que pode ser usado para limitar os OIDs disponíveis. Quando os OIDs estão incluídos na exibição, todas as outras árvores MIB são negadas. O comando SNMP *view* deve ser usado em conjunto com uma lista predefinida de objetos MIB;
- Aplicar listas de controle de acesso (ACLs) prolongadas para impedir que computadores não autorizados acessem o dispositivo. O acesso a dispositivos com permissão de leitura e/ou gravação SNMP deve ser rigorosamente controlado. Se o monitoramento e o gerenciamento de mudanças forem feitos através de *software* separado, eles devem estar em dispositivos separados;

  Segregar o tráfego SNMP em uma rede de gerenciamento separada. O tráfego da rede de gerenciamento deve estar fora de banda; no entanto, se o gerenciamento do dispositivo deve coincidir com a atividade de rede padrão, todas as comunicações que ocorram sobre essa rede devem usar alguma capacidade de criptografia. Se o dispositivo de rede tiver uma porta de gerenciamento dedicada, deve ser o único link para serviços como SNMP, *Secure Shell* (SSH), etc; e
- Mantenha as imagens do sistema e o software atualizados.

5. Referências

- **https://www.ietf.org/rfc/rfc2233.txt**
- **https://www.us-cert.gov/ncas/alerts/TA17-156A**

Brasília-DF, 23 de outubro de 2017.

Equipe do CTIR Gov