Departamento de Segurança da Informação e Comunicações – **DSIC** - *dsic.planalto.gov.br/*
Centro de Tratamento de Incidentes de Redes do Governo – **CTIR Gov** - *www.ctir.gov.br/*

Alerta nº 07/2018 - Vulnerabilidade em equipamentos *Mikrotik*.

Data de Atualização: 23/08/2018
Data de Publicação: 23/08/2018

1. Descrição

Pesquisadores (*MalwareHunter* e Simon Kenin) identificaram um ataque que utiliza vulnerabilidade no *MikroTik RouterOS* que permite sequestrar o tráfego do computador de usuários para minerar criptomoeda. A vulnerabilidade permite acesso como *root* à porta do *MikroTik RouterOS*. Após o acesso, o atacante altera a configuração do *RouterOS* para injetar um script de mineração de critpomoedas *Coinchive*.

Embora o fabricante tenha publicado um *patch* para essa falha, muitos usuários não realizaram a atualização correspondente.

2. Sistemas Afetados

- Microtik RouterOS 6,29 a 6,43rc3 (incluído).

3. Impacto

Esta vulnerabilidade, se explorada corretamente permite:

- Uso excessivo de processamento do CPU para mineração de criptomoeda;
- Participação em *Botnets* maliciosas;
- Alteração das configurações DNS dos roteadores infectados e usá-los como proxies, para dar suporte às outras campanhas de *malware*;
- Redirecionamento para páginas falsas; e
- Sequestro de dados.

4. Recomendações

- Seguir as orientações do fabricante (https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router)
- Restaurar a configuração para uma versão confiável, ou restaurar a configuração de fábrica (https://mikrotik.com/documentation/manual_2.5/System/Backup.html);
- Atualizar para a versão de *firmware* mais recente possível (https://mikrotik.com/download)
- Habilitar a proteção de senha em roteadores e dispositivos conectados;
- Substituir as senhas padrões de fábrica por senhas de elevado grau de segurança, que mesclem caracteres alfanuméricos e especiais, podendo haver letras maiúsculas e minúsculas;
- Habilitar o *firewall* para proteção adicional e usar o protocolo de segurança Acesso Protegido de *Wi-Fi II (WPA2)*;
- Remover protocolos de gerência não utilizados;
- Restringir protocolos de gerência apenas aos endereços permitidos; e
- Verificar regularmente as configurações DNS para identificar qualquer atividade suspeita na rede.

5. Referências

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847
- https://nvd.nist.gov/vuln/detail/CVE-2018-14847
- https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router
- https://www.techtudo.com.br/dicas-e-tutoriais/2018/08/roteadores-mikrotik-sao-alvos-de-ataque-no-brasil-veja-como-se-proteger.ghtml
- http://dsic.planalto.gov.br/legislacao/RequisitosMnimosSIparaAPF.pdf