TLP: CLEAR

BOLETIM DE SEGURANÇA

Moxa alerta sobre vulnerabilidades em roteadores industriais

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall

heimdall
security research
A DIVISION OF ISH

SUMÁRIO

1 INFORMAÇÕES SOBRE AS VULNERABILIDADES

O fornecedor Moxa, especializado em soluções de comunicação e redes industriais, emitiu um alerta sobre duas vulnerabilidades, uma de alta gravidade e outra crítica, que afetam diversos modelos de seus **Cellular Routers**, **Secure Routers** e **Network Security Appliances**. Essas vulnerabilidades permitem que invasores remotos obtenham privilégios de root em dispositivos comprometidos, possibilitando a execução de comandos arbitrários, o que pode resultar na execução de códigos maliciosos.

Os dispositivos da Moxa são amplamente utilizados em ambientes industriais que operam sistemas de automação e controle, principalmente nos setores de **transporte**, **energia**, **serviços públicos** e **telecomunicações**.

A empresa publicou um comunicado urgente detalhando as duas falhas identificadas:

- **CVE-2024-9138**: Uma vulnerabilidade classificada como alta, a qual envolve o uso de credenciais embutidas no sistema, permitindo que um usuário autenticado eleve privilégios e obtenha acesso root ao dispositivo.
- **CVE-2024-9140**: Essa falha foi classificada como crítica e possibilita que invasores manipulem caracteres especiais para contornar restrições de entrada, o que pode levar à execução de comandos não autorizados. Essa vulnerabilidade é particularmente preocupante, pois pode ser **explorada remotamente.**

Conforme observado, a segunda falha apresenta um risco maior devido à possibilidade de exploração sem a necessidade de acesso físico ao dispositivo.

2 RECOMENDAÇÕES

Recomenda-se reduzir ao máximo a exposição da rede, evitando que o dispositivo fique acessível diretamente pela Internet. É importante restringir o acesso SSH apenas a IPs e redes consideradas confiáveis, configurando regras específicas por meio de firewalls ou wrappers TCP. Além disso, a implementação de sistemas de detecção (IDS) ou de prevenção de intrusões (IPS) é uma medida eficaz para identificar e bloquear tentativas de exploração, uma vez que esses mecanismos monitoram o tráfego de rede em busca de possíveis sinais de ataque.

A Moxa desenvolveu soluções para lidar com vulnerabilidades identificadas em seus produtos. As atualizações e recomendações específicas para cada série de dispositivos estão listadas a seguir:

Série de produtos	Soluções
EDR-810 Series	Atualizar para a versão do firmware 3.14 ou mais nova
EDR-8010 Series	Atualizar para a versão do firmware 3.14 ou mais nova
EDR-G902 Series	Atualizar paraa versão do firmware 3.14 ou mais nova
EDR-G903 Series	Atualizar paraa versão do firmware 3.14 ou mais nova
EDR-G9004 Series	Atualizar paraa versão do firmware 3.14 ou mais nova
EDR-G9010 Series	Atualizar paraa versão do firmware 3.14 ou mais nova
EDF-G1002-BP Series	Atualizar paraa versão do firmware 3.14 ou mais nova
NAT-102 Series	Um patch oficial ou atualização de firmware não está disponível para este produto no momento. Siga as orientações acima para reduzir ao máximo a exposição da rede.
OnCell G4302-LTE4 Series	Entrar em contato com o Suporte Técnico Moxa para o patch de segurança
TN-4900 Series	Entrar em contato com o Suporte Técnico Moxa para o patch de segurança

Apenas os dispositivos mencionados acima foram identificados como vulneráveis. A Moxa assegura que as seguintes séries de produtos **não são impactadas** por essas falhas de segurança:

- **Série MRC-1002**
- **Série TN-5900**
- **Série OnCell 3120-LTE-1**

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Moxa**
- **CVE**

4 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH