BOLETIM DE SEGURANÇA

Falha de segurança crítica permite acesso não autorizado a dispositivos da Rockwell Automation

heimdall
security research
A DIVISION OF ISH

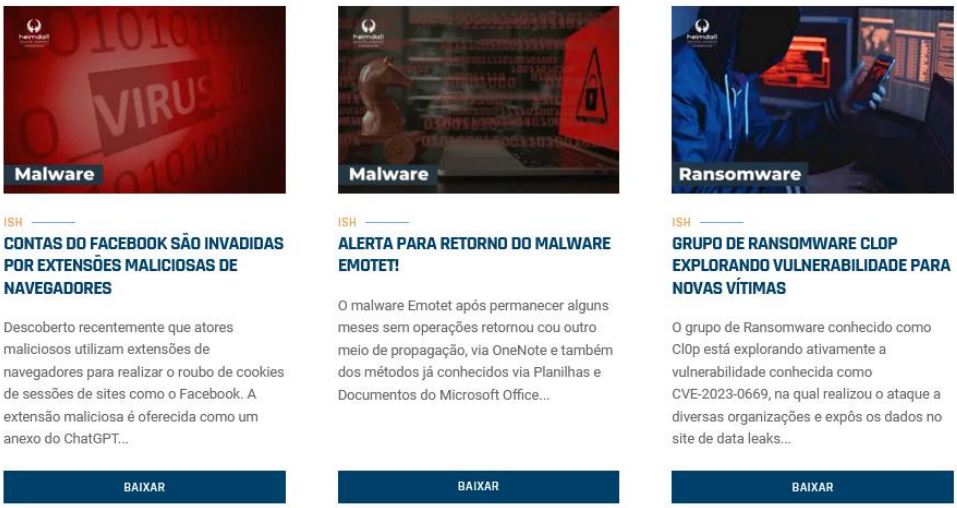
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

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



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente foi alertado sobre uma falha de segurança CVE-2024-6242 categorizada como alta nos dispositivos ControlLogix 1756 da Rockwell Automation, a qual, pode ser explorada para executar comandos de configuração e programação através do Protocolo Industrial Comum (CIP).

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-6242 afeta todos os slots conectados via backplane e permite a geração de um pacote CIP que será roteado por meio de uma placa confiável antes de chegar à CPU. O método envolve “saltar” entre slots de backplane locais dentro de um chassi 1756 usando roteamento CIP, permitindo ultrapassar o limite de segurança que deveria proteger a CPU de placas não confiáveis. Segundo a especificação CIP, a CPU verifica apenas o último slot e não toda a cadeia de slots. Isso nos permitiu ignorar a proteção Trusted Slot e nos comunicar com a CPU através de uma placa de rede não confiável.

Um invasor com acesso à rede interna pode explorar essa vulnerabilidade para ignorar a restrição de segurança e enviar comandos elevados para a CPU do PLC, como comandos de download e upload e atualizações para a CPU do controlador. Os dispositivos ControlLogix 1756 são uma série de controladores de automação programáveis da Rockwell Automation, parte da família ControlLogix, projetada para aplicações de automação industrial escaláveis e de alto desempenho. O 1756 é geralmente um componente de chassi que serve como um gabinete modular que abriga vários módulos de E/S, controladores e processadores de comunicação.

Figura 1 – Módulo de rack de chassi de 7 slots Rockwell Automation 1756 ControlLogix.

Como a maioria dos produtos industriais da Rockwell, os dispositivos ControlLogix 1756 se comunicam por CIP, um protocolo de comunicação usado em redes industriais para facilitar a troca de dados entre dispositivos. O chassi 1756 contém slots que são conectados e se comunicam por meio do backplane, uma placa de circuito impresso que conecta os vários módulos dentro do chassi, permitindo que eles se comuniquem.

Quando um operador se comunica com um CLP ControlLogix 1756, na maioria dos casos, ele se comunica pelo protocolo CIP com a placa de CPU que está conectada ao mesmo backplane no mesmo chassi que a placa de rede. Descobriu-se uma vulnerabilidade em um recurso de segurança de chassi local chamado de slot confiável, que é projetado para negar comunicação não confiável de placas de rede não confiáveis no plano do chassi. Foi encontrado uma vulnerabilidade que permitia que um invasor ignorasse o recurso de slot confiável, saltando entre slots de backplane locais dentro de um chassi 1756 usando roteamento CIP, atravessando o limite de segurança destinado a proteger a CPU de placas não confiáveis. Um invasor com esse tipo de acesso seria capaz de enviar comandos elevados, como baixar lógica para a CPU do PLC, mesmo se o invasor estiver localizado atrás de uma placa de rede não confiável.

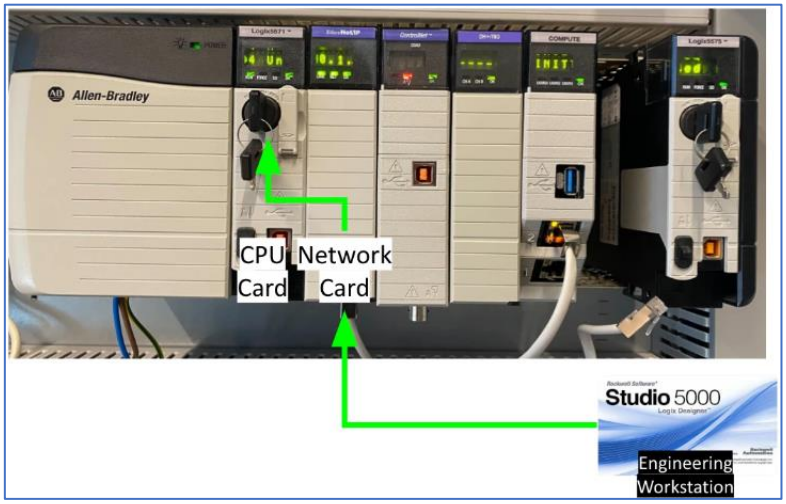


Figura 2 – Esquema básico de uma estação de trabalho de engenharia Studio 5000.

O roteamento CIP foi desenvolvido para suportar a arquitetura do sistema ControlLogix. No CIP, a ideia de um “caminho” é crucial, pois define a sequência de dispositivos e objetos de comunicação que uma mensagem ou solicitação percorre. Um caminho no CIP traça a rota de um dispositivo de origem (como um controlador em rede) para um dispositivo de destino (como um módulo de E/S). No sistema ControlLogix, os slots do backplane são identificados por uma estrutura de caminho única. Esta estrutura determina como acessar cada slot, definindo a rota de comunicação através do backplane. Cada slot no chassi 1756 possui um número de slot exclusivo. O protocolo CIP permite especificar um número de slot no caminho para alcançar um módulo específico.

O protocolo CIP utiliza o esquema de endereçamento de backplane para facilitar a comunicação entre o controlador e os módulos em diferentes slots. Definindo o caminho correto, é possível instruir o controlador a enviar ou receber dados de um slot específico no backplane.

Um exemplo de caminho pode ser: **1,3,1,0 - Backplane (01), Cartão 3 (03), Backplane (01), Cartão 0 (00)**.

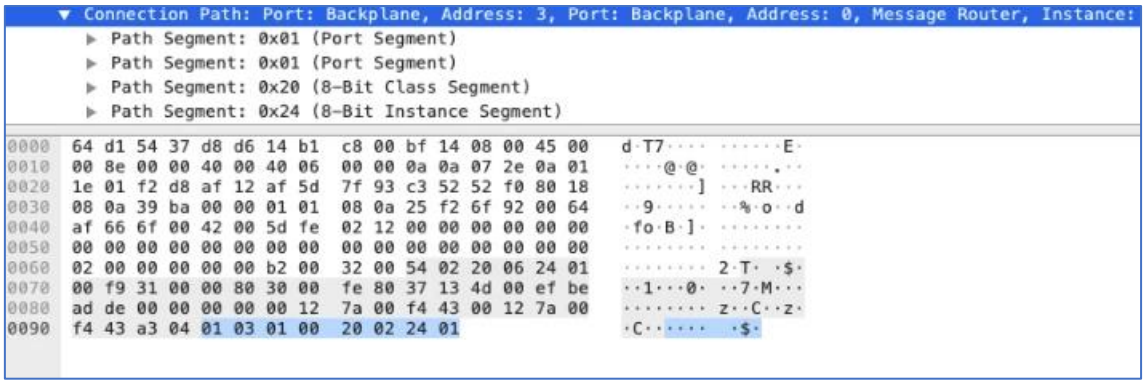


Figura 3 – Captura de tela do Wireshark mostrando um caminho CIP.

Em uma linha de produção, um PLC 1756 pode se conectar a múltiplas fontes através de diversas placas de rede, como o painel HMI, estação de trabalho de engenharia, entre outros. Para assegurar que somente dispositivos específicos realizem operações avançadas no PLC, como o download de lógica, foi introduzido um mecanismo de segurança denominado “trusted slot”. Esse recurso auxilia na criação e implementação de políticas de segurança dentro do chassi ControlLogix, garantindo que apenas slots autorizados possam se comunicar entre si, protegendo contra acessos não autorizados e possíveis adulterações.

Com o recurso de slot confiável ativado, o controlador rejeita comunicações por caminhos não confiáveis. Isso exige autenticação no módulo para que qualquer indivíduo acesse o controlador com software de programação. Um módulo específico pode ser designado como um slot confiável, permitindo que ele se comunique livremente com outros slots dentro do mesmo chassi, principalmente com a CPU.

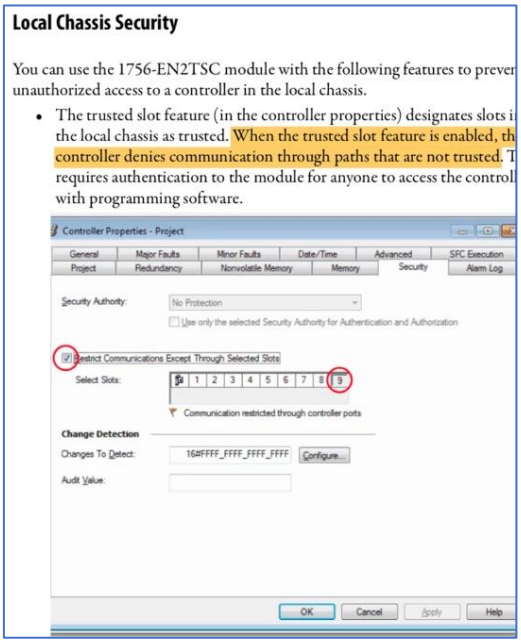


Figura 4 – Chassi local do Rockwell.

Se a segurança estiver ativada, mas a nossa placa de rede não for confiável, a CPU recusará aceitar operações avançadas de qualquer tráfego CIP originado da placa de rede não confiável.

Para aumentar a segurança e ajudar na identificação de futuras vulnerabilidades semelhantes, foi implementando uma nova regra no Snort para detectar o comportamento específico de “jump”. O Snort, um sistema de código aberto para detecção de intrusões em redes, passará a incluir uma regra que monitora e identifica tentativas de explorar o protocolo CIP. Esta regra auxiliará as organizações a identificar e reagir a possíveis ameaças de segurança de maneira mais eficiente. A regra do Snort que foi implementada buscará qualquer solicitação de encaminhamento de CIP aberta onde o caminho solicitado tenha dois ou mais redirecionamentos de chassi local no mesmo backplane do PLC.

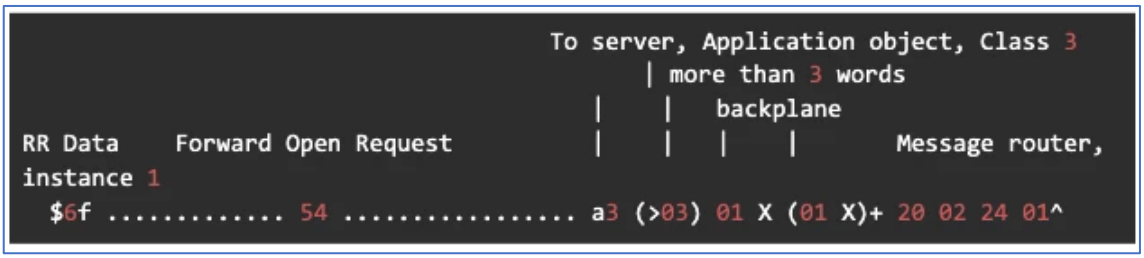


Figura 5 – Regra SNORT.

3 RECOMENDAÇÕES

A Rockwell emitiu uma correção para CVE-2024-6242, e os usuários devem aplicá-la imediatamente. **A CISA também publicou um comunicado** com orientações de mitigação.

Segundo informações da Rockwell, essa vulnerabilidade impacta os módulos de E/S ControlLogix, GuardLogix e 1756 ControlLogix nas seguintes versões:

- ControlLogix: Version V28
- GuardLogix: Version V31
- 1756-EN4TR: Version V2
- 1756-EN2T, Series A/B/C (unsigned version): Version v5.007
- 1756-EN2F, Series A/B (unsigned version): Version v5.007
- 1756-EN2TR, Series A/B (unsigned version): Version v5.007
- 1756-EN3TR, Series B (unsigned version): Version v5.007
- 1756-EN2T, Series A/B/C (signed version): Version v5.027
- 1756-EN2F, Series A/B (signed version): Version v5.027
- 1756-EN2TR, Series A/B (signed version): Version v5.027
- 1756-EN3TR, Series B (signed version): Version v5.027
- 1756-EN2T, Series D: Version V10.006
- 1756-EN2F, Series C: Version V10.009
- 1756-EN2TR, Series C: Version V10.007
- 1756-EN3TR, Series B: Version V10.007
- 1756-EN2TP, Series A: Version V10.020

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Claroty
- Thehackernews
- NVD

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH