TLP: CLEAR

BOLETIM DE SEGURANÇA

Exploração ativa afeta dispositivos Zyxel CPE devido à vulnerabilidade CVE-2024-40891

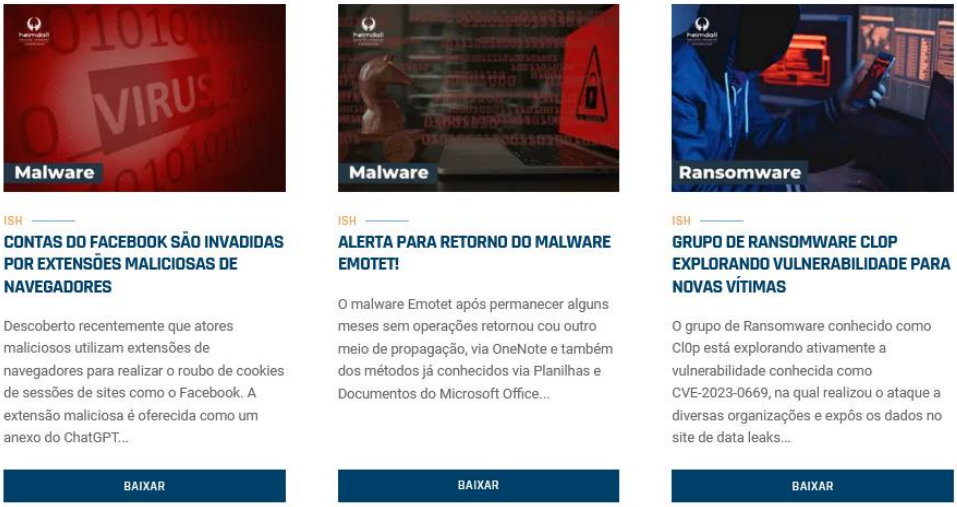
heimdall
security research

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



SUMÁRIO

LISTA DE TABELAS

1 INTRODUÇÃO EXECUTIVA

Uma vulnerabilidade de injeção de comandos, identificada como **CVE-2024-40891**, foi descoberta nos dispositivos da série **Zyxel CPE**. Esta falha está sendo ativamente explorada por atacantes, permitindo a execução de comandos arbitrários que podem comprometer totalmente o sistema, resultando em exfiltração de dados ou infiltração na rede. Até o momento, não há patches disponíveis para mitigar essa vulnerabilidade.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A **CVE-2024-40891** é uma vulnerabilidade de injeção de comandos que permite a execução de comandos arbitrários nos dispositivos afetados. Ela é semelhante à **CVE-2024-40890**, com a diferença principal de que a **CVE-2024-40891** é baseada em Telnet, enquanto a **CVE-2024-40890** é baseada em HTTP. Ambas as vulnerabilidades permitem que atacantes não autenticados executem comandos utilizando contas de serviço.

Dados obtidos pela GreyNoise indicam que as tentativas de exploração da vulnerabilidade partiram de múltiplos endereços IP, sendo que a maioria deles está registrada em Taiwan. Também relatam que há sinais claros de que os agentes maliciosos estão tentando explorar a vulnerabilidade em massa e destaca que algumas variantes do **botnet Mirai** já adicionaram a capacidade de explorar CVE-2024-40891 após identificar uma "sobreposição significativa entre IPs que exploram CVE-2024-40891 e aqueles classificados como Mirai".

2.1 SISTEMAS E PRODUTOS AFETADOS

A vulnerabilidade afeta os dispositivos da série Zyxel CPE, especificamente o modelo *VMG4325-B10A* com a versão de firmware *1.00(AAFR.4)C0_20170615*.

2.2 IMPACTO DA VULNERABILIDADE

Os principais impactos da vulnerabilidade nos dispositivos Zyxel CPE incluem:

- Execução remota de comandos
- Comprometimento total do dispositivo
- Exfiltração de dados sensíveis
- Infiltração na rede interna
- Criação de backdoors persistentes
- Uso em botnets e ataques distribuídos
- Interrupção de serviços e instabilidade da rede

3 RECOMENDAÇÕES

Para minimizar os riscos associados a essa vulnerabilidade é essencial que as organizações adotem as seguintes medidas de segurança:

Monitoramento de tráfego

- Filtrar o tráfego em busca de requisições HTTP incomuns direcionadas às interfaces de gerenciamento dos dispositivos Zyxel CPE.

Restrição de acesso

- Restringir o acesso às interfaces administrativas dos dispositivos a endereços IP confiáveis.

Acompanhar atualizações da Zyxel

- Fique atento aos comunicados de segurança da Zyxel e aplique patches ou mitigações imediatamente após serem disponibilizados.

Desativação de serviços não utilizados

- Desativar serviços como Telnet e HTTP se não forem necessários para a operação do dispositivo.
- Desative funcionalidades de gerenciamento remoto que não estejam em uso para reduzir a superfície de ataque.

Monitoramento contínuo

- Implementar soluções de monitoramento contínuo para detectar atividades suspeitas ou anômalas nos dispositivos.

4 INDICADORES DE COMPROMETIMENTO (IOC)

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de IPs

Indicadores de IPs	
IP	59.126.139[.]160 114.33.109[.]78 114.46.127[.]117 220.134.253[.]157 150.116.64[.]139 125.229.163[.]166 114.35.165[.]165 61.220.216[.]233 114.32.249[.]227 114.34.31[.]203

Tabela 1 – Indicadores de Comprometimento de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **GreyNoise**
- **The Hacker News**

6 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH