BOLETIM DE SEGURANÇA

Zyxel alerta sobre falha crítica de injeção de comando em seus produtos

heimdall
security research
A DIVISION OF ISH

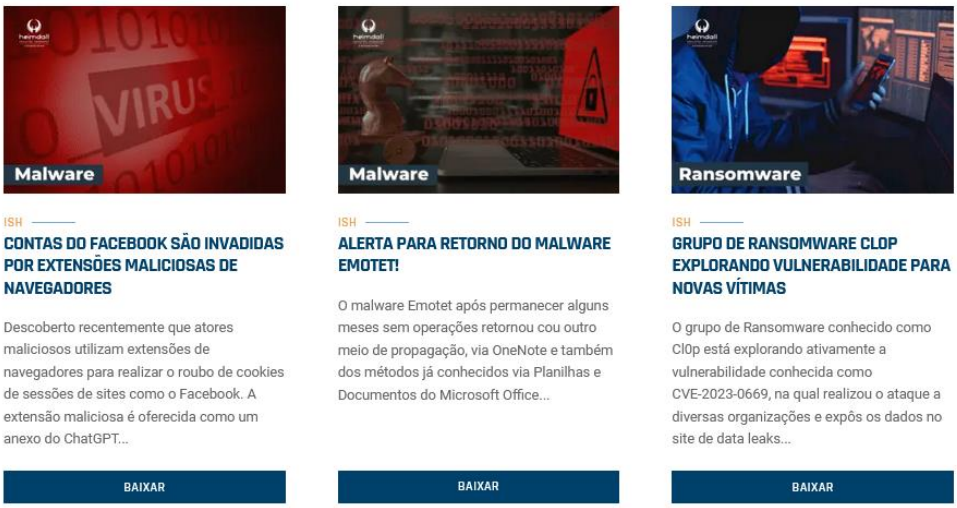
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

A Zyxel divulgou atualizações de segurança para resolver uma vulnerabilidade crítica presente em diversos modelos de seus roteadores empresariais, que pode permitir a execução de comandos no sistema operacional por invasores não autenticados. Identificada como CVE-2024-7261, a falha recebeu uma pontuação CVSS v3 de **9,8 (crítica)**. O problema ocorre devido à validação inadequada de entradas, resultante de um tratamento incorreto dos dados fornecidos pelo usuário, o que possibilita que invasores remotos executem comandos arbitrários no sistema operacional afetado. A falha na neutralização de elementos especiais no parâmetro 'host' do programa CGI em certas versões de APs e roteadores de segurança pode permitir que invasores não autenticados executem comandos do sistema operacional ao enviar um cookie manipulado para um dispositivo vulnerável, comunicou a Zyxel.

2 PRODUTOS E VERSÕES AFETADAS

Os Acess Points (APs) da Zyxel afetados

- **Série NWA:** NWA50AX, NWA50AX PRO, NWA55AXE, NWA90AX, NWA90AX PRO, NWA110AX, NWA130BE, NWA210AX, NWA220AX-6E | Todas as versões até 7.00 são vulneráveis. **Atualize para 7.00 (ABYW.2) e posterior**
- **NWA1123-AC PRO** | Todas as versões até 6.28 são vulneráveis. **Atualize para 6.28 (ABHD.3) e posterior**
- **NWA1123ACv3, WAC500, WAC500H** | Todas as versões até 6.70 são vulneráveis. **Atualize para 6.70 (ABVT.5) e posterior**
- **Série WAC: WAC6103D-I, WAC6502D-S, WAC6503D-S, WAC6552D-S, WAC6553D-E** | Todas as versões até 6.28 são vulneráveis. **Atualize para 6.28(AAXH.3) e posteriores**
- **Série WAX: WAX300H, WAX510D, WAX610D, WAX620D-6E, WAX630S, WAX640S-6E, WAX650S, WAX655E** | Todas as versões até 7.00 são vulneráveis. **Atualize para 7.00 (ACHF.2) e posterior**
- **Série WBE: WBE530, WBE660S** | Todas as versões até 7.00 são vulneráveis. **Atualize para 7.00 (ACLE.2) e posterior**

A Zyxel diz que o roteador de segurança ***USG LITE 60AX*** executando ***V2.00(ACIP.2)*** também é afetado, mas este modelo é atualizado automaticamente pela nuvem para V2.00(ACIP.3), que implementa o patch para CVE-2024-7261.

3 CONCLUSÃO

A atualização contra vulnerabilidades em dispositivos Zyxel é essencial para garantir a segurança das redes corporativas, atores maliciosos frequentemente exploram falhas conhecidas em firewalls, roteadores e dispositivos de acesso remoto dessa marca para comprometer sistemas, roubar dados sensíveis e realizar ataques em larga escala. Organizações que não corrigem essas vulnerabilidades podem ser alvos de ransomware, espionagem cibernética ou sequestro de dispositivos para redes botnets, a aplicação de patches de segurança e o monitoramento contínuo são medidas cruciais para mitigar esses riscos, mantendo a integridade e disponibilidade dos sistemas empresariais.

4 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

- **Restringir o acesso remoto**, se possível, desative o acesso remoto aos dispositivos vulneráveis.
- **Segurança de rede**, implementar firewalls e filtros de tráfego para restringir o acesso não autorizado a partir de redes externas, bloqueando IPs suspeitos ou desconhecidos de se conectar aos roteadores.
- **Monitoramento e análise de log**, monitore o tráfego da rede e examine regularmente os logs de acesso para identificar tentativas de exploração ou atividades incomuns.
- **Desativar funções não utilizadas**, se houver funcionalidades nos roteadores que não são utilizadas, desative-as para reduzir a superfície de ataque potencial.
- **Segmentação de rede**, mantenha os roteadores em segmentos de rede isolados e use VLANs para minimizar o risco de comprometimento da rede como um todo.
- **Revisar contas de usuários**, assegure-se de que as credenciais dos dispositivos estejam seguras, usando senhas fortes e revisando regularmente a lista de contas de usuários com permissões de acesso.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Zyxel**
- **Bleepingcomputer**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH