BOLETIM DE SEGURANÇA

Novas vulnerabilidades em Firewall Zyxel

heimdall
security research
A DIVISION OF ISH

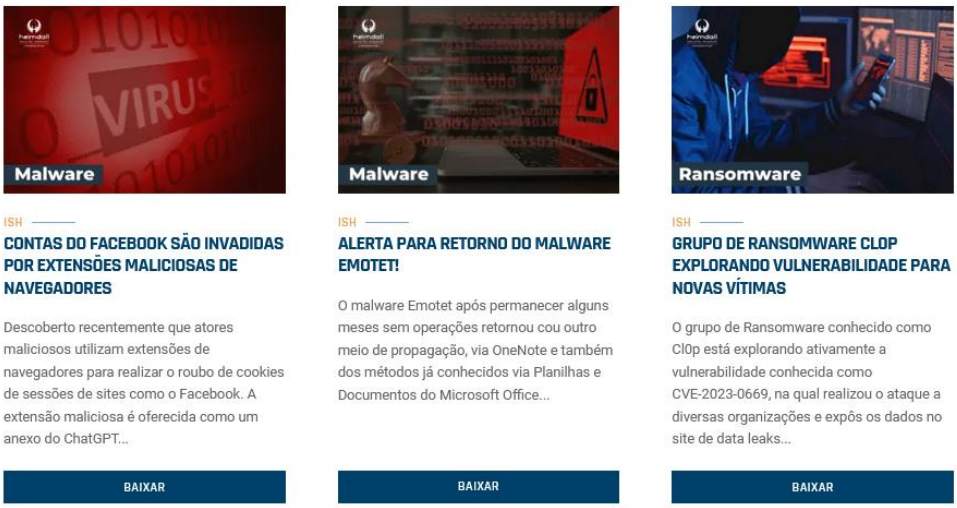
TLP: CLEAR

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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Zyxel lançou um comunicado para correção de segurança que abordam múltiplas vulnerabilidades em algumas versões de firewall e ponto de acesso (AP), sendo uma dela um problema de execução remota não autorizada de código. A mesma informa que os usuários são aconselhados a instalar os patches para proteção ideal.

Figura 1 – Logo da Zyxel Networks.

2 VULNERABILIDADES INFORMADAS E DETALHES

Segue todos os detalhes sobre as vulnerabilidade informadas e corrigidas pela Zyxel em sua atualização de segurança.

CVE-2023-6397

- Uma vulnerabilidade de desreferência de ponteiro nulo em algumas versões de firewall pode permitir que um invasor baseado em LAN cause condições de **negação de serviço** (DoS) baixando um arquivo compactado RAR criado em um host do lado da LAN se o firewall tiver o "Anti-Malware" recurso habilitado.

CVE-2023-6398

- Vulnerabilidade de **injeção de comando pós-autenticação** no binário de upload de arquivo em algumas versões de firewall e AP pode permitir que um invasor autenticado com privilégios de administrador execute alguns comandos do sistema operacional (SO) em um dispositivo afetado via FTP.

CVE-2023-6399

- Uma vulnerabilidade de string de formato em algumas versões de firewall pode permitir que um usuário VPN IPSec autenticado cause condições DoS contra o daemon "deviceid" enviando um nome de host criado para um dispositivo afetado se ele tiver o recurso "Device Insight" ativado.

CVE-2023-6764

- Uma vulnerabilidade de cadeia de formato em uma função do recurso VPN IPSec em algumas versões de firewall poderia permitir que um invasor conseguisse **execução remota não autorizada de código**, enviando uma sequência de cargas úteis especialmente criadas contendo um ponteiro inválido; entretanto, tal ataque exigiria conhecimento detalhado do layout e configuração da memória de um dispositivo afetado.

A classificação de gravidade das vulnerabilidade acima variam de média a alta, conforme seus riscos.

3 PRODUTOS E VERSÕES AFETADOS

Abaixo segue imagem e tabela disponibilizadas com produtos e versões afetadas pelas vulnerabilidades.

Série de firewall	Versão afetada				Disponibilidade de patches
	CVE-2023-6397	CVE-2023-6398	CVE-2023-6399	CVE-2023-6764	
ATP	ZLD V4.32 a V5.37 Patch 1	ZLD V4.32 a V5.37 Patch 1	ZLD V5.10 a V5.37 Patch 1	ZLD V4.32 a V5.37 Patch 1	ZLD V5.37 Patch 2
USG FLEX	ZLD V4.50 a V5.37 Patch 1	ZLD V4.50 a V5.37 Patch 1	ZLD V5.10 a V5.37 Patch 1	ZLD V4.50 a V5.37 Patch 1	ZLD V5.37 Patch 2
USG FLEX 50(W)/USG20(W)-VPN	Não afetado	ZLD V4.16 a V5.37 Patch 1	ZLD V5.10 a V5.37 Patch 1	ZLD V4.16 a V5.37 Patch 1	ZLD V5.37 Patch 2
USG FLEX H	Não afetado	iOS V1.10 a V1.10 Patch 1	iOS V1.10 a V1.10 Patch 1	Não afetado	Hotfix disponível* Patch padrão do uOS V1.20 em abril de 2024

Figura 2 – Firewalls afetados por CVE-2023-6397, CVE-2023-6398, CVE-2023-6399 e CVE-2023-6764.

Modelo de AP	Versão afetada	Disponibilidade de patches
NWA50AX	6.29(ABYW.3) e anteriores	6.29(ABYW.4)
NWA55AXE	6.29(ABZL.3) e anteriores	6,29(ABZL.4)
NWA90AX	6.29(ACCV.3) e anteriores	6.29(ACCV.4)
NWA110AX	6,65 (ABTG.1) e anteriores	6,70(ABTG.2)
NWA210AX	6,65 (ABTD.1) e anteriores	6,70(ABTD.2)
NWA220AX-6E	6,65 (ACCO.1) e anteriores	6,70(ACCO.1)
NWA1123ACv3	6,65 (ABVT.1) e anteriores	6,70(ABVT.1)
WAC500	6,65(ABVS.1) e anteriores	6,70(ABVS.1)
WAC500H	6,65 (ABWA.1) e anteriores	6,70(ABWA.1)
CERA300H	6,60(ACHF.1) e anteriores	6,70(ACHF.1)
CERA510D	6,65 (ABTF.1) e anteriores	6,70(ABTF.2)
CERA610D	6,65(ABTE.1) e anteriores	6,70(ABTE.2)
CERA620D-6E	6,65 (ACCN.1) e anteriores	6,70(ACCN.1)

CERA630S	6,65(ABZD.1) e anteriores	6,70(ABZD.2)
CERA640S-6E	6,65 (ACCM.1) e anteriores	6,70(ACCM.1)
CERA650S	6,65(ABRM.1) e anteriores	6,70(ABRM.2)
CERA655E	6,65 (ACDO.1) e anteriores	6,70(ACDO.1)
WBE660S	6,65(ACGG.1) e anteriores	6,70(ACGG.2)
NWA50AX-PRO	6,65(ACGE.1) e anteriores	O hotfix está disponível mediante solicitação*
		Patch padrão 6.80(ACGE.0) em julho de 2024
NWA90AX-PRO	6,65 (ACGF.1) e anteriores	O hotfix está disponível mediante solicitação*
		Patch padrão 6.80(ACGF.0) em julho de 2024

Tabela 1 – APs afetados pelo CVE-2023-6398.

4 CONCLUSÃO

A correção de vulnerabilidades em produtos Zyxel tornou-se uma prioridade crítica para organizações em todo o mundo. Estes dispositivos, amplamente utilizados em redes corporativas, são frequentemente o alvo de atores maliciosos que procuram explorar falhas de segurança para ganhar acesso não autorizado a dados sensíveis. A importância de atualizar e corrigir esses produtos não pode ser subestimada, pois uma única brecha pode resultar em danos significativos, incluindo perda de dados, interrupções operacionais e danos à reputação. Além disso, a correção proativa dessas vulnerabilidades demonstra um compromisso com a segurança cibernética, protegendo não apenas os ativos da empresa, mas também a confiança dos clientes e parceiros.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Zyxel**
- **NVD**

heimdall
security research
A DIVISION OF ISH