BOLETIM DE SEGURANÇA

Falhas em dispositivos D-LINK deixam milhares de dispositivos vulneráveis a ataques de malware

heimdall
security research
A DIVISION OF ISH

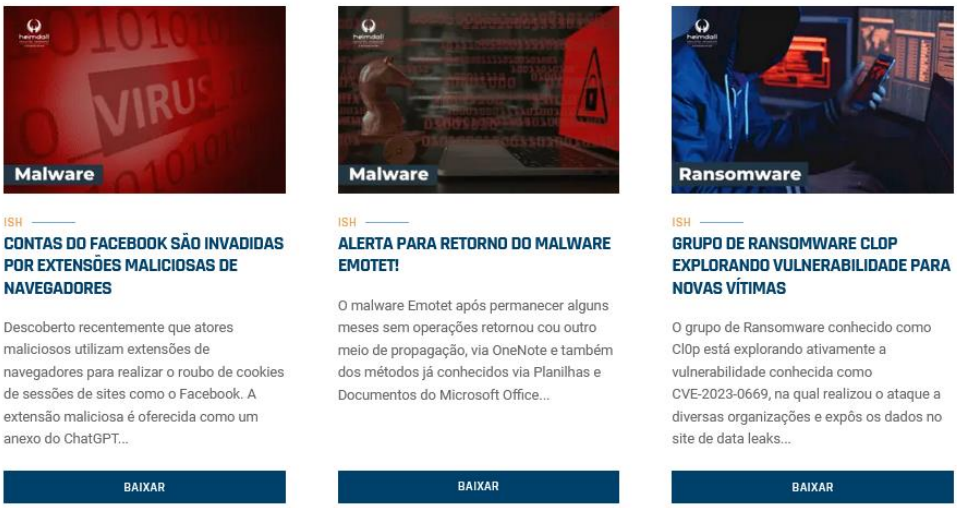
TLP: CLEAR

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, atores de ameaças estão explorando ativamente duas falhas de segurança em milhares de dispositivos D-Link Network Attached Storage (**NAS**). Essas vulnerabilidades, rastreadas são como CVE-2024-3272 categorizada como crítica e CVE-2024-3273 categorizada com alta, impactam os produtos legados da D-Link que já atingiram o status de fim de vida (EoL).

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As vulnerabilidades CVE-2024-3272 e CVE-2024-3273 tem como objetivo afetar os dispositivos D-Link DNS-320L, DNS-325, DNS-327L e DNS-340L, impactando o processamento do arquivo `/cgi-bin/nas_sharing.cgi` no componente HTTP GET Request Handler. Sendo que a primeira realiza a manipulação do argumento user com o messagebus de entrada leva a credenciais embutidas em código iniciando o ataque remotamente. A segunda tem como objetivo a manipulação dos argumentos do sistema levando à uma execução remota de código (**RCE**).

De acordo com a empresa de inteligência de ameaças GreyNoise, os atores estão tentando transformar as vulnerabilidades em armas para a entrega da botnet mirai.

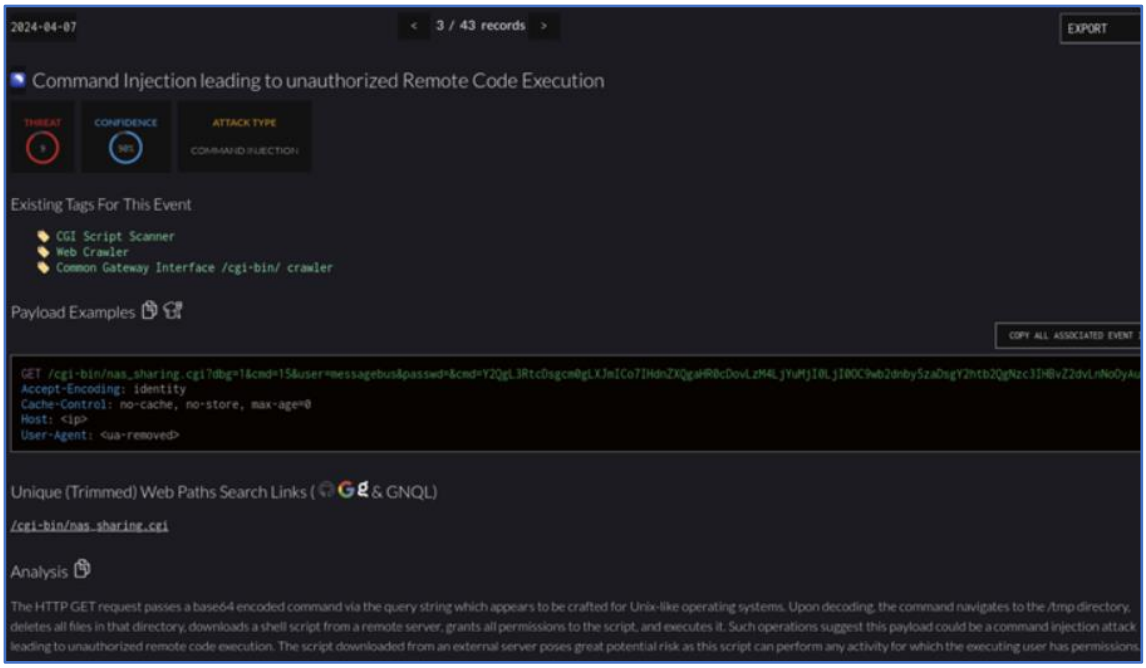


Figura 1 – Análise realizada pela GreyNoise.

Descobertas recentes reforçam a capacidade da botnet Mirai de se adaptarem e incorporarem novas vulnerabilidades em seu repertório. Os agentes da ameaça estão ágeis na criação de variantes específicas para explorar essas vulnerabilidades e comprometer o maior número possível de dispositivos.

Com a mudança no cenário de ataques, com os dispositivos de rede se tornando alvos frequentes de invasores com motivações financeiras e ligações a Estados-nação, destaca-se que os atores de ameaças estão migrando cada vez mais para ataques de varredura iniciados por malware. Esses ataques têm como objetivo identificar vulnerabilidades nas redes-alvo, ampliando ainda mais o desafio de segurança cibernética.

Quando invasores lançam ataques de varredura a partir de hosts comprometidos, eles têm objetivos específicos em mente, permitindo que cubram seus rastros usando hosts comprometidos como intermediários, dificultando a rastreabilidade de suas atividades maliciosas, contornando as delimitações geográficas ao escolherem hosts comprometidos em diferentes locais geográficos permitindo evitar detecções e restrições baseadas em localização. Eles também aproveitam recursos, em que os dispositivos comprometidos fornecem recursos computacionais adicionais, permitindo que os invasores gerem um volume maior de solicitações de varredura. Os hosts comprometidos podem ser recrutados para ampliar botnets, aumentando assim o poder de ataque e a capacidade de disseminação de malware.

Em uma exploração bem-sucedida, invasor pode executar comandos arbitrários no sistema, potencialmente levando ao acesso não autorizado a informações confidenciais, à modificação das configurações do sistema ou às condições de negação de serviço.

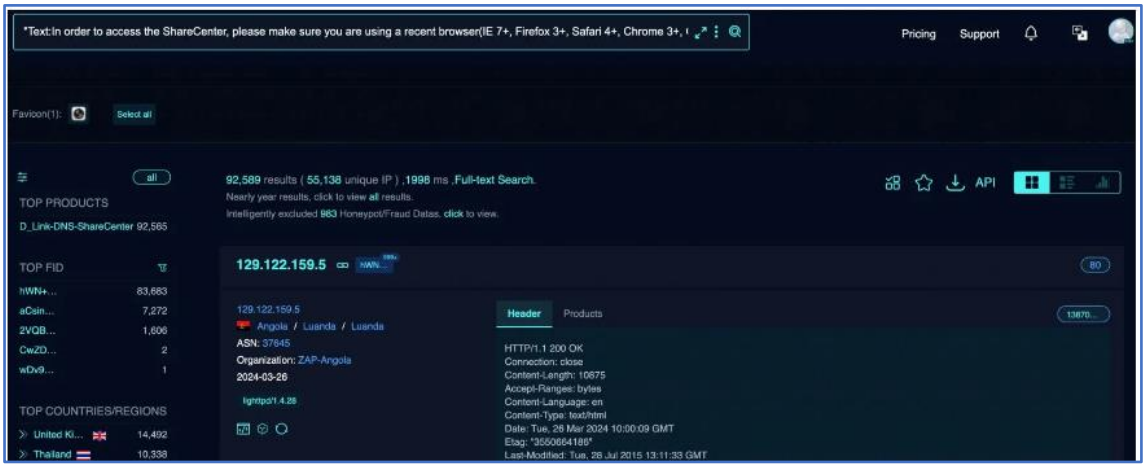


Figura 2 – Dispositivos D-Link NAS vulneráveis expostos.

De acordo com o porta-voz da D-Link, todo armazenamento ligado à rede D-Link está obsoleto e fora de serviço há anos. Os recursos associados a esses produtos não são mais desenvolvidos nem suportados, informando também, que os dispositivos NAS não possuem atualização on-line automática ou recursos de entrega de alertas, tornando impossível notificar os proprietários sobre esses ataques em andamento.

3 DISPOSITIVOS EXPOSTOS ONLINE

A Shadowserver divulgou em sua página no Twitter-X, que também está monitorando a CVE-2024-3273, em sua primeira publicação é possível notar um mapa com instâncias vulneráveis encontradas, conforme mostra imagem abaixo.

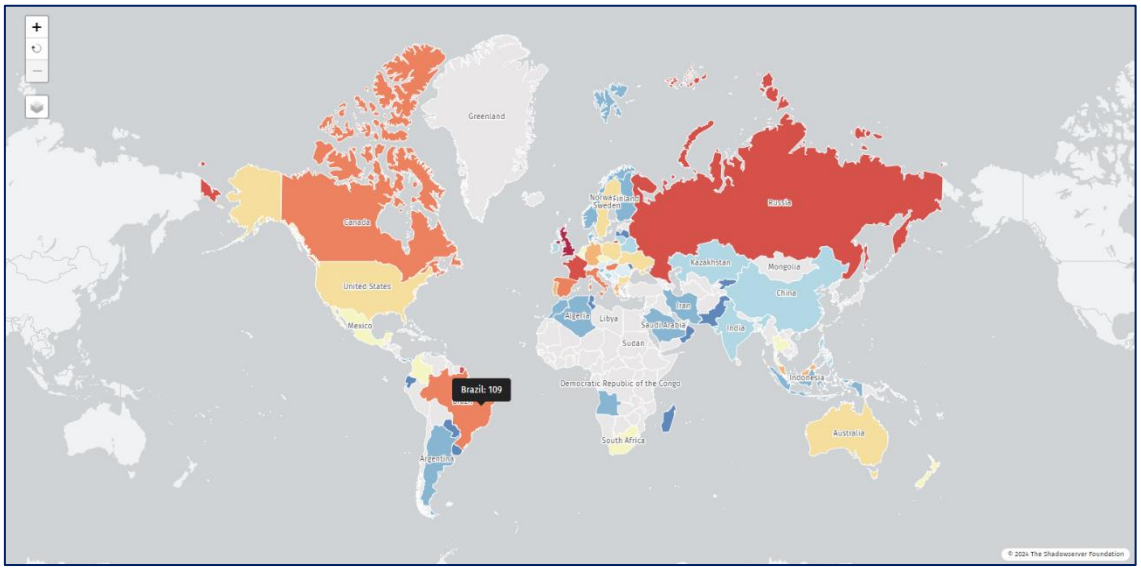


Figura 3 – Dispositivos D-Link NAS vulneráveis expostos - Shadowserver.

Na imagem acima é possível observar alguns dispositivos vulneráveis associado ao Brasil, o quais requerem uma devida atenção por seus administradores.

Em outra publicação é mostrado o rastreamento de tentativas de exploração D-Link CVE-2024-3273 (incluindo tentativas de propagação de botnets do tipo Mirai), diz a mesma.

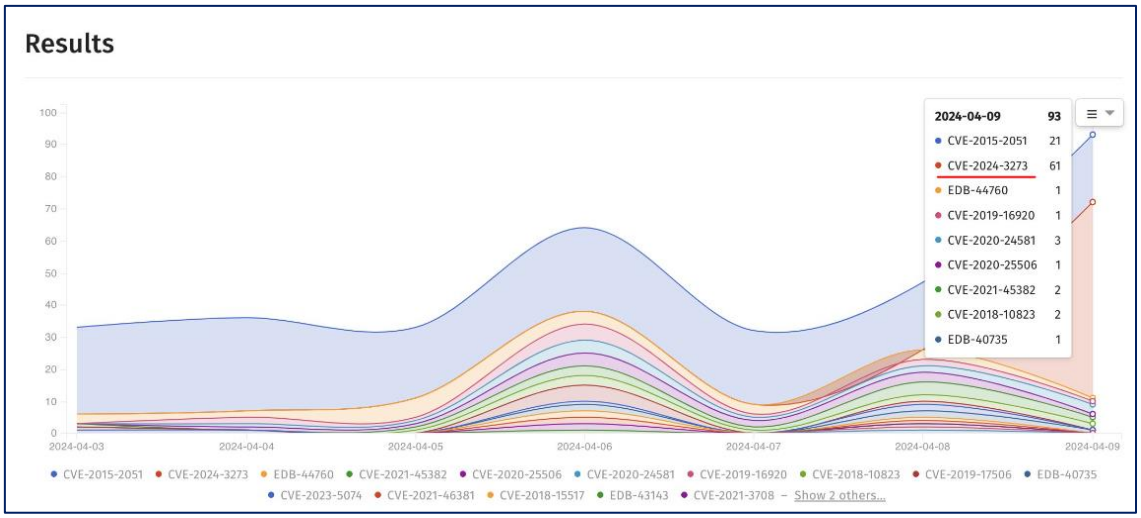


Figura 4 – Explorações observadas - Shadowserver.

4 RECOMENDAÇÕES

Abaixo são elencadas pela ISH, medidas que poderão ser adotadas visando a mitigação da referida vulnerabilidades, como por exemplo:

D-Link NAS CVE-2024-3272 (RCE)

- Verifique se o seu dispositivo está afetado visitando o site da D-Link.
- Aplique as atualizações de firmware mais recentes com urgência.
- Mesmo após a correção, altere as senhas padrão do seu dispositivo NAS.

D-Link NAS CVE-2024-3273 (Injeção de Comandos)

- Utilize ativos de segurança, como firewalls e anti-malware, sempre atualizados.
- Implemente uma política de mínimo privilégio para restringir ações na rede aos usuários conforme suas funções organizacionais.
- Bloqueie o tráfego da porta 445/SMB para fora da rede até que as atualizações sejam instaladas.
- Considere usar o recurso de grupo de usuários protegidos do Active Directory para contas de administradores de domínio.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- D-Link
- Thehackernews
- Bleepingcomputer
- Shadowserver
- GreyNoise

heimdall
security research
A DIVISION OF ISH