BOLETIM DE SEGURANÇA

TP-Link soluciona vulnerabilidade crítica que permitia controle remoto no roteador de jogos C5400X

heimdall
security research
A DIVISION OF ISH

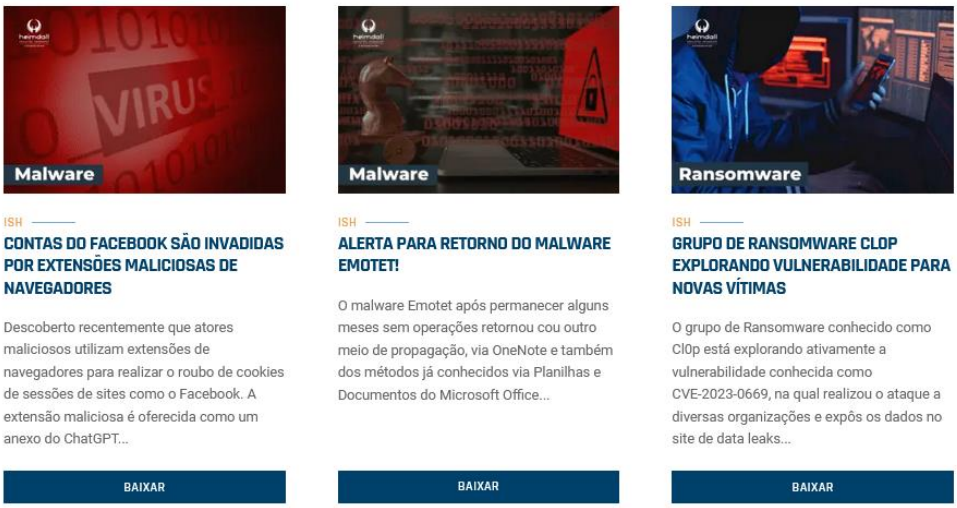
TLP: CLEAR

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 a TP-Link corrigiu uma falha de segurança critica com pontuação máxima no CVSS, CVE-2024-5035, no roteador de jogos **TP-Link Archer C5400X**, a qual foi apontada por pesquisadores de segurança e podendo pode levar à execução remota de código em dispositivos suscetíveis, enviando solicitações especialmente criadas.

2 DETALHES SOBRE A VULNERABILIDADE

O problema reside no binário “rftest”, que abre brechas para injeção de comandos e overflow de buffer nas portas TCP 8888, 8889 e 8890. Este binário é responsável por operar um serviço de autoavaliação da interface sem fio e tarefas associadas. Explorando essa brecha, um invasor pode enviar mensagens manipuladas através dessas portas, potencialmente permitindo a execução de comandos arbitrários com privilégios elevados. Este tipo de ataque explora os metacaracteres de shell, que são caracteres especiais usados para controlar funções em shells de linha de comando, mas que podem ser utilizados de forma maliciosa quando a entrada do usuário não é devidamente filtrada para prevenir ações não autorizadas.

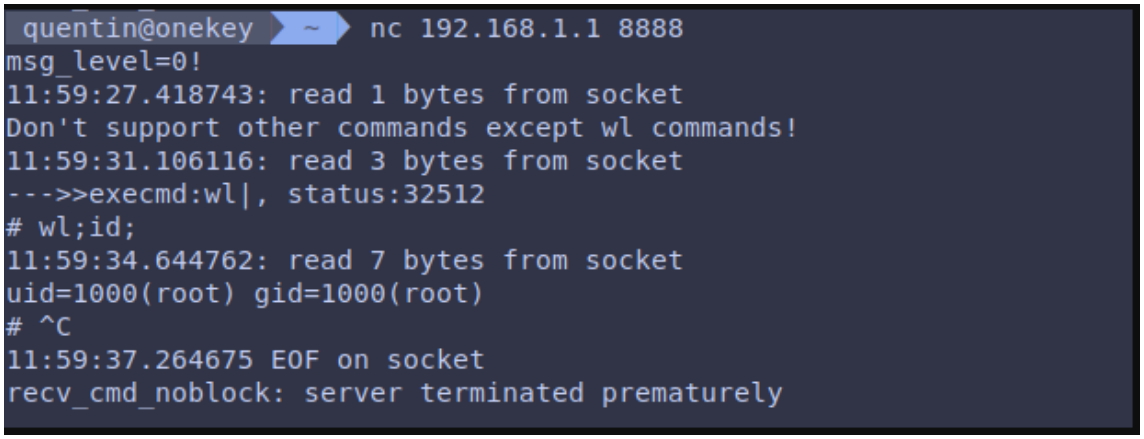


Figura 1 – Injeção de ID de comando através da porta 8888.

- **Versão vulnerável a falha**: <= 1_1.1.6
- **Versão corrigida**: 1_1.1.7

3 CONCLUSÃO

Os roteadores TP-LINK, amplamente utilizados em ambientes domésticos e empresariais, apresentam vulnerabilidades significativas que podem ser exploradas por atores maliciosos. Falhas comuns incluem senhas padrão fracas, firmware desatualizado e configuração inadequada, que abrem portas para ataques de força bruta e injeção de comandos. Atores maliciosos frequentemente exploram essas vulnerabilidades para comprometer a segurança da rede, roubar informações sensíveis e lançar ataques DDoS. A falta de atualizações regulares de segurança agrava o problema, tornando os roteadores um alvo atraente para cibercriminosos. A adoção de práticas de segurança robustas, como a atualização frequente do firmware e a utilização de senhas fortes, é crucial para mitigar esses riscos.

4 RECOMENDAÇÕES

Recomendamos que os usuários façam o download da atualização do firmware diretamente do portal oficial da TP-Link ou utilizem o painel de administração do roteador para realizar a atualização. Nos mais as medidas abaixo também podem ser utilizadas para uma melhor proteção.

Alteração de senhas padrão

- Modifique as senhas padrão do roteador para algo forte e único. Evite senhas fáceis de adivinhar e utilize uma combinação de letras, números e caracteres especiais.

Configuração de segurança da rede Wi-Fi

- Utilize o protocolo de segurança WPA3, se disponível, ou WPA2 como alternativa. Desative o WPS (Wi-Fi Protected Setup), que pode ser explorado por atacantes.

Segmentação de redes

- Separe a rede principal da rede de convidados para limitar o acesso de dispositivos não confiáveis à sua rede interna. Isso pode ser feito configurando VLANs (Redes Locais Virtuais).

Desativação de serviços não necessários

- Desative serviços e funções que não são utilizados, como UPnP (Universal Plug and Play), para reduzir a superfície de ataque.

Monitoramento e logs

- Ative o registro de logs no roteador para monitorar atividades suspeitas e revisá-las regularmente. Isso pode ajudar a identificar e responder rapidamente a possíveis tentativas de invasão.

Restrição de acesso remoto

- Desative o acesso remoto ao painel de administração do roteador ou limite-o a endereços IP específicos de confiança. Isso impede que atacantes acessem seu roteador a partir de locais remotos.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **TP-LINK**
- **Onekey**
- **NVD**
- **Bleepingcomputer**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH