DrayTek alerta sobre bug de execução remota de código em roteadores Vi

Data: 2025-10-02 19:45:49

Autor: Inteligência Against Invaders

A fabricante de hardware de rede DrayTek divulgou um comunicado para alertar sobre uma

vulnerabilidade de segurança em vários modelos de roteadores Vigor que poderia permitir que

atores remotos e não autenticados executassem código arbitrário.

A falha, rastreada identificada como CVE-2025-10547, foi relatada ao fornecedor em 22 de julho pelo pesquisador de segurança da ChapsVision, Pierre-Yves Maes.

“A vulnerabilidade pode ser acionada quando invasores remotos não autenticados enviam solicitações HTTP ou HTTPS criadas para a interface do usuário da Web (WebUI) do dispositivo”, lê o aviso de segurança da DrayTek.

“A exploração bem-sucedida pode causar corrupção de memória e falha do sistema, com o potencial de permitir a execução remota de código em certas circunstâncias.”

A DrayTek observou que a exposição da WAN pode ser reduzida desativando o acesso remoto à VPN WebUI/SSL ou restringindo-o com ACLs/VLANs. No entanto, a WebUI permanece acessível pela LAN, exposta a invasores locais.

Maes disse ao BleepingComputer que a causa raiz do CVE-2025-10547 é um valor de pilha não inicializado que pode ser aproveitado para causar o *livre()*para operar em locais de memória arbitrários, também conhecidos como *arbitrário free()*, para obter a execução remota de código (RCE).

O pesquisador testou com sucesso suas descobertas criando um exploit e executando-o em dispositivos DrayTek.

O boletim de segurança da DrayTek não menciona a exploração contínua, mas é recomendável mitigar o risco.

Abaixo estão os modelos afetados pelo CVE-2025-10547 e o destino de atualização de versão de firmware recomendado para mitigar a falha:

- Vigor1000B, Vigor2962, Vigor3910/3912 ? 4.4.3.6 ou posterior (alguns modelos 4.4.5.1)
- Vigor2135, Vigor2763/2765/2766, Vigor2865/2866 Series (incl. LTE & 5G), Vigor2927 Series (incl. LTE & 5G) ? 4.5.1 ou posterior
- Vigor2915 Series ? 4.4.6.1 ou posterior
- Série Vigor2862/2926 (incl. LTE) ? 3.9.9.12 ou posterior
- Vigor2952/2952P, Vigor3220 ? 3.9.8.8 ou posterior
- Série Vigor2860/2925 (incl. LTE) ? 3.9.8.6 ou posterior

- Vigor2133/2762/2832 Series ? 3.9.9.4 ou posterior
- Vigor2620 Series ? 3.9.9.5 ou posterior
- VigorLTE 200n ? 3.9.9.3 ou posterior

Os roteadores DrayTek, especialmente os modelos Vigor, são muito comuns em ambientes prosumer e de pequenas e médias empresas (SMB). A lista de modelos afetados abrange uma ampla gama, desde modelos principais até roteadores mais antigos usados em ambientes DLS/telecomunicações.

Recomenda-se que os administradores de sistema apliquem as atualizações de segurança de firmware disponíveis o mais rápido possível. Maes diz que divulgará todos os detalhes técnicos do CVE-2025-10547 amanhã.

[IMAGEM REMOVIDA]