BOLETIM DE SEGURANÇA

Microsoft alerta para várias vulnerabilidades importantes no OpenVPN

heimdall
security research
A DIVISION OF ISH

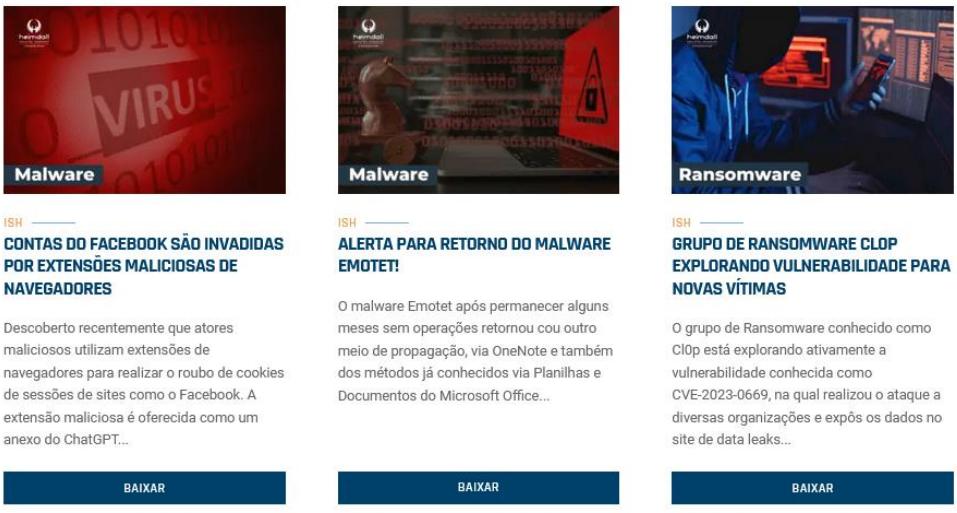
TLP: CLEAR

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

Pesquisadores da Microsoft identificaram recentemente várias vulnerabilidades importantes no OpenVPN, os invasores poderiam encadear e explorar remotamente algumas das vulnerabilidades descobertas para obter uma cadeia de ataque consistindo em execução remota de código (RCE) e escalonamento de privilégios locais (LPE). Essa cadeia de ataque poderia permitir que os invasores obtivessem controle total sobre os endpoints alvos, resultando potencialmente em violações de dados, comprometimento do sistema e acesso não autorizado a informações confidenciais.

2 ARQUITETURA DO OPENVPN

O OpenVPN é amplamente usado por milhares de empresas abrangendo vários setores em grandes plataformas, como Windows, iOS, macOS, Android e BSD. Como tal, a exploração das vulnerabilidades descobertas, que afetam todas as versões do OpenVPN **anteriores** à versão **2.6.10** e **2.5.10**, pode colocar endpoints e empresas em risco significativo de ataque.

Arquitetura do cliente do servidor OpenVPN

OpenVPN é um avançado sistema VPN projetado para criar conexões seguras ponto a ponto ou site a site, suportando configurações roteadas, em ponte e acesso remoto. Ele inclui aplicativos de cliente e servidor, oferecendo uma solução completa para comunicações seguras. A autenticação entre os pares pode ser feita por meio de chaves secretas pré-compartilhadas, certificados ou combinações de nome de usuário e senha. Em ambientes multicliente, o servidor pode emitir certificados individuais para cada cliente, utilizando assinaturas digitais robustas e uma autoridade de certificação confiável, garantindo alta segurança e integridade na autenticação e na conexão VPN.

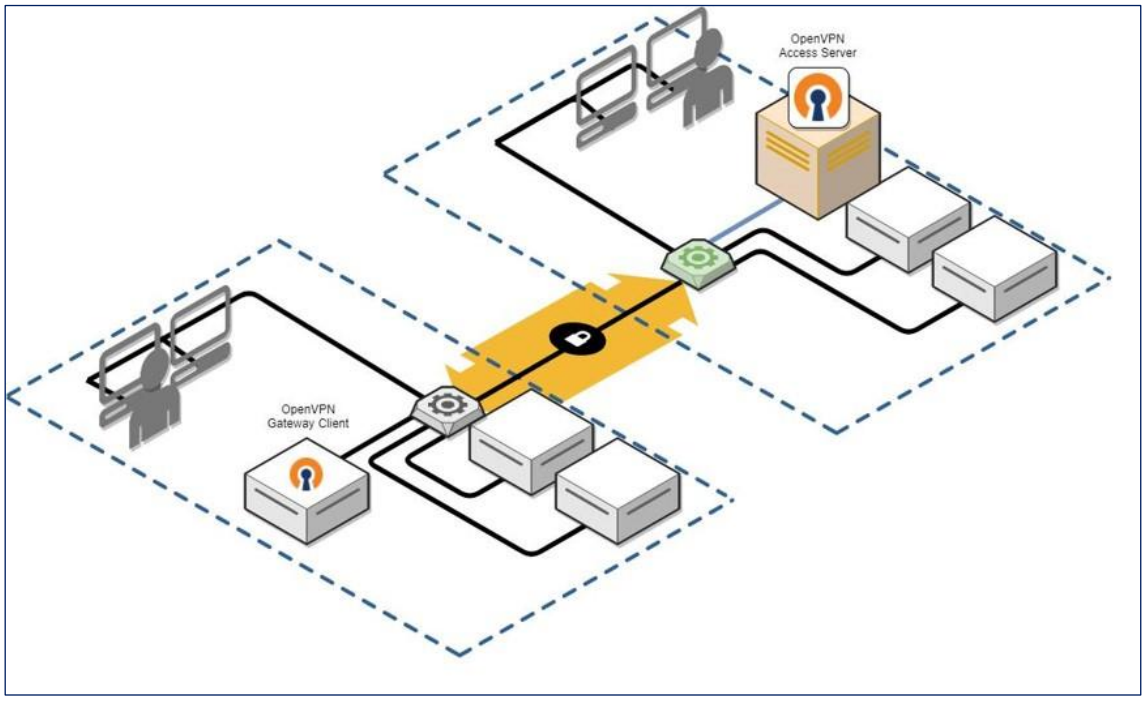


Figura 1 – Cliente-servidor OpenVPN.

Arquitetura do lado do cliente

A arquitetura do lado do cliente é onde foram descobertas três vulnerabilidades adicionais (CVE-2024-27459, CVE-2024-24974 e CVE-2024-27903), as quais serão explicadas logo mais. A arquitetura do cliente do OpenVPN pode ser resumida no seguinte diagrama simplificado:

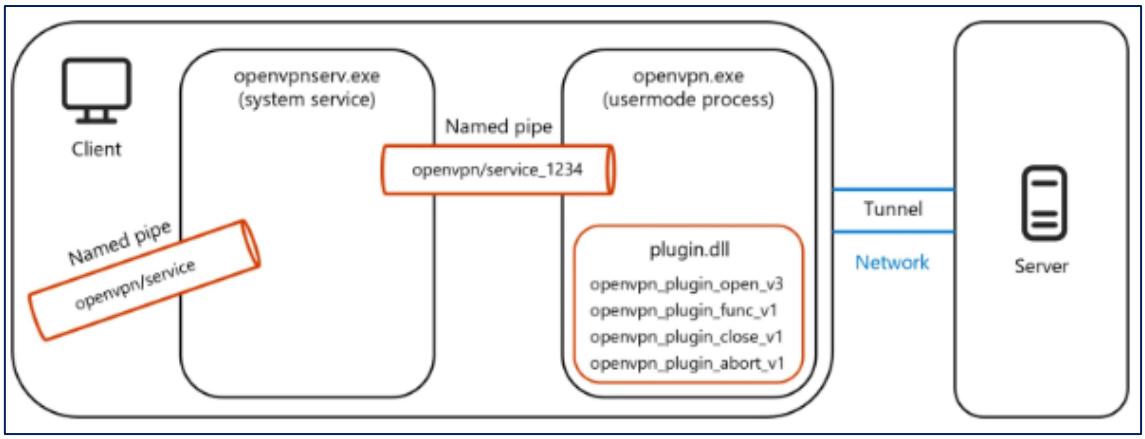


Figura 2 – Arquitetura do cliente OpenVPN com plugin.dll carregado.

openvpnserv.exe e openvpn.exe

O serviço do sistema executa comandos elevados em nome do usuário, lidando com tarefas como adicionar ou remover configurações de DNS, endereços IP e rotas, além de habilitar o Protocolo de Configuração Dinâmica de Host (DHCP). Esses comandos são enviados pelo processo openvpn.exe através de um pipe nomeado criado especificamente para comunicação entre essas duas entidades, como “openvpn/service_XXX”, onde XXX representa o ID do thread (TID) que é passado para o processo recém-criado como um argumento na linha de comando. Os comandos recebidos são estruturados em um formato binário que contém as informações relevantes para o comando específico. Essa estrutura é validada antes de o comando apropriado ser executado. A figura abaixo mostra um exemplo da estrutura que contém informações para adicionar ou remover a configuração de DNS:

```
typedef struct {
    message_header_t header;
    interface_t iface;
    char domains[512];
    short family;
    int addr_len;
    inet_address_t addr[4]; /* support up to 4 dns addresses */
} dns_cfg_message_t;
```

Figura 3 – Estrutura de gerenciamento de configuração de DNS OpenVPN.

Além disso, openvpnserv.exe serve como unidade de gerenciamento, gerando processos openvpn.exe mediante solicitações de diferentes usuários na máquina. Isso pode ser feito automaticamente usando a GUI do OpenVPN ou enviando solicitações especificamente criadas. A comunicação para esse processo ocorre por meio de um segundo pipe nomeado, como “openvpn/service”.

Openvpn .exe é o processo de modo de usuário sendo gerado em nome do cliente. Quando openvpn.exe inicia, ele recebe um caminho para um arquivo de

configuração (como um argumento de linha de comando). O arquivo de configuração fornecido contém informações diferentes.

3 DETALHES SOBRE AS VULNERABILIDADES E EXPLORAÇÕES

CVE-2024-1305

Existe uma vulnerabilidade no projeto "*tap-windows6*" que está relacionada ao desenvolvimento do adaptador Terminal Access Point (TAP) utilizado pelo OpenVPN. Na pasta *src* do projeto, o arquivo device.c contém o código responsável pelo objeto do dispositivo TAP e sua inicialização. No arquivo *device.c*, o método *CreateTapDevice* inicializa um objeto de tabela de despacho com retornos de chamada para métodos que gerenciam diversos Controles de Entrada/Saída (IOCTLs) para o dispositivo. Um desses métodos é o *TapDeviceWrite*, que lida com o IOCTL de gravação.

```
// Allocate the NBL and NB. Link MDL chain to NB.
netBufferList = NdisAllocateNetBufferAndNetBufferList(
    Adapter->ReceiveNblPool,
    0,                              // ContextSize
    0,                              // ContextBackFill
    mdl==NULL?Irp->MdlAddress:mdl,  // MDL chain
    // PacketBuffer will always be from the Irp's SystemBuffer, but may be offset beyond the start.
    // This will only be the case if there is not a prefix (and mdl == NULL).
    mdl==NULL?(ULONG)(PacketBuffer-((unsigned char *)Irp->AssociatedIrp.SystemBuffer)):0,
    fullLength
    );
```

Figura 4 – Localização da vulnerabilidade de estouro de kernel.

O método *TapDeviceWrite* realiza diversas operações e, eventualmente, chama o método *TapSharedSendPacket*. Este último, por sua vez, chama *NdisAllocateNetBufferAndNetBufferLists* duas vezes. Os parâmetros *PacketLength* e *PrefixLength* são passados pelo *TapDeviceWrite* e, portanto, podem ser controlados por um invasor. Se esses valores forem suficientemente grandes, a soma deles (*fullLength*) pode ultrapassar o limite de um inteiro sem sinal de 32 bits. Esse estouro de valor resulta na alocação de um tamanho de memória menor do que o esperado, o que pode causar um problema de estouro de memória.

CVE-2024-27459

O serviço interativo no OpenVPN 2.6.9 e versões anteriores permite que um invasor envie dados, causando um estouro de pilha que pode ser usado para executar código arbitrário com mais privilégios.

O serviço *openvpnserv.exe* lerá o tamanho da mensagem em um loop infinito do processo openvpn.exe e então manipulará a mensagem recebida chamando o método *HandleMessage*. O método *HandleMessage* lê o tamanho fornecido pelo loop infinito e converte os bytes lidos no tipo relevante de acordo:

```
DWORD read;
union {
    message_header_t header;
    address_message_t address;
    route_message_t route;
    flush_neighbors_message_t flush_neighbors;
    block_dns_message_t block_dns;
    dns_cfg_message_t dns;
    enable_dhcp_message_t dhcp;
    register_ring_buffers_message_t rrb;
    set_mtu_message_t mtu;
    wins_cfg_message_t wins;
} msg;
ack_message_t ack = {
    .header = {
        .type = msg_acknowledgement,
        .size = sizeof(ack),
        .message_id = -1
    },
    .error_number = ERROR_MESSAGE_DATA
};

read = ReadPipeAsync(pipe, &msg, bytes, count, events);
if (read != bytes || read < sizeof(msg.header) || read != msg.header.size)
{
    goto out;
}

ack.header.message_id = msg.header.message_id;
```

Figura 5 – Localização da vulnerabilidade de estouro de pilha.

CVE-2024-24974

A terceira vulnerabilidade envolve acesso não privilegiado a um recurso do sistema operacional. O serviço *openvpnserv.exe* gera um novo processo *openvpn.exe* com base em solicitações de usuário recebidas por meio do pipe nomeado "*openvpn**service*". Essa vulnerabilidade permite acesso remoto ao pipe de serviço nomeado, permitindo que um invasor interaja remotamente com ele e inicie operações nele.

CVE-2024-27903

Uma vulnerabilidade no mecanismo de plugin do OpenVPN que permite que plugins sejam carregados de vários caminhos em um dispositivo endpoint. Esse comportamento pode ser explorado por invasores para carregar plugins prejudiciais desses diferentes caminhos.

Exploração e encadeamento das vulnerabilidades

Conforme a Microsoft, todas as vulnerabilidades identificadas podem ser exploradas quando um invasor obtém acesso às credenciais OpenVPN de um usuário, o que pode ser feito usando técnicas de roubo de credenciais, como comprar credenciais roubadas na dark web, usar malware para roubo de

informações ou farejar tráfego de rede para capturar hashes NTLMv2 e, em seguida, usar ferramentas de cracking como HashCat ou John the Ripper para decodificá-los.

Versões do OpenVPN afetadas

- *Versões do OpenVPN anteriores a **2.5.10** e **2.6.10***

Devido a explorações anteriores de falhas no OpenVPN por atores maliciosos, estas vulnerabilidades requerem uma notável atenção.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Initial Access	T1190 Exploit Public-Facing Application	Exploração de vulnerabilidades em serviços de acesso remoto, como o OpenVPN, para obter acesso inicial ao sistema.
Execution	T1059 Command and Scripting Interpreter	Execução de comandos e scripts maliciosos através da exploração das vulnerabilidades identificadas no OpenVPN.
Privilege Escalation	T1547 Hijack Execution Flow T1068 Exploitation for Privilege Escalation	Modificação de arquivos de inicialização e serviços para manter o acesso ao sistema comprometido. Exploração das vulnerabilidades para elevar os privilégios de um usuário normal para um administrador ou root, permitindo controle total sobre o sistema.
Defense Evasion	T1211 Exploitation for Defense Evasion	Bypass de mecanismos de segurança utilizando falhas no OpenVPN para evitar detecção e resposta.
Impact	T1499 Endpoint Denial of Service	Realização de atividades que podem levar a problemas de desempenho ou disponibilidade, como sobrecarga de recursos através da exploração das vulnerabilidades.

Tabela 1 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação das ameaças, como por exemplo:

- Aplicar imediatamente o patch relevante: OpenVPN 2.6.10.
- Certifique-se de que os clientes OpenVPN estejam desconectados da Internet e segmentados.
- Limite o acesso aos clientes OpenVPN somente a usuários autorizados.
- Reduza o risco garantindo a segmentação adequada, exigindo nomes de usuário e senhas fortes e reduzindo o número de usuários que têm autenticação de escrita.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **NVD**
- **MITRE ATT&CK**

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH