**Relatório**

**Análise de vulnerabilidades**

**Controle de Versões:**

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA** | **VERSÃO** | **AUTOR** | **ALTERAÇÕES** |
| XX/XX/XXXX | 1.0 | Analista | Versão Inicial |
|  | 1.1 |  | Revisão |
|  | 1.2 |  | Revisão Final |
|  | 1.3 |  | Versão Final |

|  |
| --- |
| ***CONFIDENCIAL*** |
| *Este documento contém informações proprietárias e confidenciais e todos os dados encontrados durante os testes e presentes neste documento foram tratados de forma a garantir a privacidade e o sigilo deles. A duplicação, redistribuição ou uso no todo ou em parte de qualquer forma requer o consentimento do* ***NOME DA EMPRESA.*** |

Sumário

[**Aviso Legal** 7](#_Toc125536589)

[**Informações de Contato** 7](#_Toc125536590)

[**Sumário Executivo** 8](#_Toc125536591)

[Introdução 9](#_Toc125536592)

[**Escopo** 9](#_Toc125536593)

[Limitações do Escopo 9](#_Toc125536594)

[Metodologia 10](#_Toc125536595)

[**Narrativa da Análise Técnica** 11](#_Toc125536596)

[Hosts encontrados ativos na rede 11](#_Toc125536597)

[Sistema TAL.exe, TAL.exe 14](#_Toc125536598)

[Sistema TAL.exe 14](#_Toc125536599)

[Sistema TAL.exe 15](#_Toc125536600)

[Possível correção 16](#_Toc125536601)

[Passo a passo para resolver essa vulnerabilidade: 16](#_Toc125536602)

[**HOST IP** 17](#_Toc125536603)

[*Coleta de Informações* 17](#_Toc125536604)

[Vetores de Ataques Conhecidos 18](#_Toc125536605)

[Possível correção 19](#_Toc125536606)

[**HOST IP** 20](#_Toc125536607)

[*Coleta de informações* 20](#_Toc125536608)

[Vetores de Ataques Conhecidos 20](#_Toc125536609)

[Porta 22 - OpenSSH 20](#_Toc125536610)

[Possível correção 21](#_Toc125536611)

[**HOST IP** 22](#_Toc125536612)

[*Coleta de informações* 22](#_Toc125536613)

[Vetores de Ataques Conhecidos 23](#_Toc125536614)

[Porta 443 - PRTG 23](#_Toc125536615)

[Logjam 24](#_Toc125536616)

[Possível correção 24](#_Toc125536617)

[Slowloris DOS attack 25](#_Toc125536618)

[Possível correção 26](#_Toc125536619)

[Bypass through ftp helper 26](#_Toc125536620)

[Possível correção 26](#_Toc125536621)

[**HOST IP** 28](#_Toc125536622)

[*Coleta de informações* 28](#_Toc125536623)

[Vetores de Ataques Conhecidos 29](#_Toc125536624)

[Possível correção 29](#_Toc125536625)

[**HOST IP** 30](#_Toc125536626)

[*Coleta de informações* 30](#_Toc125536627)

[Vetores de Ataques Conhecidos 31](#_Toc125536628)

[Possível correção 31](#_Toc125536629)

[**HOST IP** 32](#_Toc125536630)

[*Coleta de informações* 32](#_Toc125536631)

[Vetores de Ataques Conhecidos 32](#_Toc125536632)

[Possível correção 32](#_Toc125536633)

[**HOST IP** 33](#_Toc125536634)

[*Coleta de informações* 33](#_Toc125536635)

[Vetores de Ataques Conhecidos 33](#_Toc125536636)

[Possível correção 33](#_Toc125536637)

[**HOST IP** 34](#_Toc125536638)

[*Coleta de informações* 34](#_Toc125536639)

[Vetores de Ataques Conhecidos 35](#_Toc125536640)

[Possível correção 35](#_Toc125536641)

[**HOST IP** 36](#_Toc125536642)

[*Coleta de informações* 36](#_Toc125536643)

[Vetores de Ataques Conhecidos 37](#_Toc125536644)

[Porta 80 | 5357 | 5985 37](#_Toc125536645)

[Slowloris DOS attack 39](#_Toc125536646)

[Possível correção 39](#_Toc125536647)

[**HOST IP** 40](#_Toc125536648)

[*Coleta de informações* 40](#_Toc125536649)

[Vetores de Ataques Conhecidos 41](#_Toc125536650)

[Possível correção 41](#_Toc125536651)

[**HOST IP** 42](#_Toc125536652)

[*Coleta de informações* 42](#_Toc125536653)

[Vetores de Ataques Conhecidos 42](#_Toc125536654)

[Possível correção 42](#_Toc125536655)

[**HOST IP** 43](#_Toc125536656)

[*Coleta de informações* 43](#_Toc125536657)

[Vetores de Ataques Conhecidos 43](#_Toc125536658)

[Porta 22 - OpenSSH 43](#_Toc125536659)

[Possível correção 44](#_Toc125536660)

[**Considerações Finais** 45](#_Toc125536661)

Índice Figuras

[Figure 1 - Ferramenta nbtscan,, informações sobre a rede. 14](#_Toc125536703)

[Figure 2 - Sistema TAL.exe. 15](#_Toc125536704)

[Figure 3 - Sistema TAL.exe 15](#_Toc125536705)

[Figure 4 - Possível Correção sistemas TAL. 16](#_Toc125536706)

[Figure 5 – Evidência - Porta ssh v. 7.4 (Aberta). 17](#_Toc125536707)

[Figure 6 - Evidência Firewall Bypass 24](#_Toc125536708)

# **Aviso Legal**

A análise foi realizada durante o período de **XX/XX/XXXX** até **XX/XX/XXXX**. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período.

O trabalho desenvolvido pelo Analista tem como objetivo fazer um levantamento dos riscos e recomendar formas para minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa, testada antes de serem implementadas no ambiente em produção. O analista **não se responsabiliza** pela não correção e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços de terceiros.

# **Informações de Contato**

|  |  |
| --- | --- |
|  |  |

|  |  |  |
| --- | --- | --- |
| **NOME** | **CARGO** | **INFORMAÇÕES** |
| **NOME EMPRESA** | | |
| NOME GERENTE | Gerente geral da empresa | **Telefone:** (00) 0 0000-0000  **Email:** email@email.com |
| **CORPO TÉCNICO | NOME EMPRESA** | | |
| ANALISTA | Analista de Vulnerabilidade | **Telefone:** (00) 0 0000-0000  **Email:** email@email.com |
| NOME GESTOR | Gestor de Ti | **Telefone:** (00) 0 0000-0000  **Email:** email@email.com |

# **Sumário Executivo**

O Analista avaliou a postura de segurança da EMPRESA através de uma Análise Interna pelo período de 16 de janeiro de 2023 até 25 de janeiro de 2023. Os resultados das avaliações efetuadas no ambiente a partir da intranet demonstram que a empresa possui riscos cibernéticos com a presença de vulnerabilidades de nível **CRÍTICO** que **comprometem a integridade, disponibilidade e o sigilo** **de informações** **sensíveis**.

É altamente recomendável que o NOME DA EMPRESA resolva as vulnerabilidades classificadas como risco crítico com **alta prioridade** para que não haja um impacto negativo para os negócios, visto a criticidade das vulnerabilidades encontradas e passíveis de serem exploradas através da internet.

## Introdução

O Analista conduzirá uma avaliação de segurança (*Análise de Vulnerabilidade*) no ambiente digital do NOME EMPRESA.

A avaliação foi conduzida de maneira a simular um ciberataque a partir de uma invasão por acesso remoto com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **integridade, disponibilidade e confidencialidade** das informações da empresa.

Os testes foram realizados entre os dias 16 de janeiro de 2023 e 25 de janeiro de 2023 e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

# **Escopo**

|  |  |
| --- | --- |
| **TIPO DE AVALIAÇÃO** | **DETALHES** |
| Pentest White Box Interno | Conhecimento de toda a rede interna da EMPRESA |

A avaliação escolhida foi do tipo ***White Box (com conhecimento de todas as informações)***, com uma observação. O Analista se “passará” por atacante infiltrado na rede via acesso remoto, onde, um colaborador clicou em um link malicioso ou aceitou um acesso remoto.

## Limitações do Escopo

As limitações impostas pela Empresa é que não seja realizado teste de intrusão nos servidores de ip IP.

## Metodologia

Para execução destes trabalhos, o Analista adotou a metodologia própria mesclada com padrões existentes e solidamente reconhecidos, tais como *PTES* *(Penetration Testing Execution Standard) e OWASP Top Ten nas quais foram* executados nas seguintes fases:

* Coleta de Informações
* Varredura
* Enumeração
* ~~Exploração~~
* ~~Pós Exploração~~
* Documentação

A fase de coleta de informações tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de ip, subdomínios e ambientes digitais de propriedade da Empresa.

A fase de varredura consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

A fase de enumeração permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser uteis para o sucesso de um ataque.

~~A fase de exploração tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.~~

~~A fase de pós exploração tem como objetivo aprofundar o ataque obtendo mais privilégios e aumentando o nível de acesso, se deslocando para outros sistemas a fim de controlar ou extrair dados mais sensíveis.~~

A fase de documentação consiste em relatar todos os resultados obtidos nas fases anteriores.

# **Narrativa da Análise Técnica**

Os testes iniciaram no dia **XX/XX/XXXX** de posse apenas do bloco de ip.

**O bloco de ip enumerado é IP/24 ou /16 ou /32 ou IP 1-254**

## Hosts encontrados ativos na rede

|  |  |  |  |
| --- | --- | --- | --- |
| Legenda: Marca de seleção com preenchimento sólido Não foi encontrado vulnerabilidade pública  Fechar com preenchimento sólido Vulnerabilidade pública encontrada | | | |
| IP | Nome do Host | Vulnerável? | Nível |
| IP | NOME DOS HOSTS | Fechar com preenchimento sólido | Alto |
| IP | NOME DOS HOSTS | Fechar com preenchimento sólido | Alto |
| IP | NOME DOS HOSTS | Fechar com preenchimento sólido | Critico |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Fechar com preenchimento sólido | Critico |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Marca de seleção com preenchimento sólido | Baixo |
| IP | NOME DOS HOSTS | Fechar com preenchimento sólido | Critico |

|  |
| --- |
| **BLOCO DE IP** |
| IP /24 – 16 - 32 |

Figure 1 - Ferramenta nbtscan,, informações sobre a rede.

### Sistema TAL.exe, TAL.exe

Ao analisar os sistemas sendo executado na máquina, verifiquei que o sistema Escriba é o único sistema que não está com o PED Habilitado.

Prevenção de Execução de Dados (PED, na sigla em inglês) é uma técnica de segurança utilizada para evitar a execução de código malicioso em um sistema. Ela é frequentemente implementada como uma característica de segurança em sistemas operacionais e geralmente é habilitada por padrão.

Se a função PED estiver desabilitada, isso pode permitir que um atacante execute código malicioso no sistema, possivelmente levando a um comprometimento completo do sistema. Alguns dos vetores de ataques comuns que podem ser usados para explorar essa vulnerabilidade incluem buffer overflow, injeção de código e exploração de vulnerabilidades de aplicativos.

### Sistema TAL.exe

Tabela

Descrição gerada automaticamente com confiança média

Figure 2 - Sistema TAL.exe.

### Sistema TAL.exe

Interface gráfica do usuário, Tabela

Descrição gerada automaticamente

Figure 3 - Sistema TAL.exe

## Possível correção

Figure 4 - Possível Correção sistemas TAL.

Para mitigar essa vulnerabilidade, é recomendável habilitar a função PED no sistema operacional e manter todos os aplicativos atualizados com as últimas correções de segurança. Além disso, é importante usar software de segurança, como firewalls e programas antivírus, para detectar e bloquear tentativas de ataques.

### Passo a passo para resolver essa vulnerabilidade:

Verificar se a função PED está habilitada no sistema operacional

Atualizar todos os softwares e aplicativos instalados no sistema

Instalar e manter atualizado software de segurança, como firewalls e antivírus

Configurar a segurança de rede adequadamente para bloquear tentativas de ataques

Monitorar o sistema regularmente para detectar qualquer atividade suspeita.

Se necessário, contratar uma equipe de segurança especializada para ajudar na identificação e correção de vulnerabilidades de segurança.

# **HOST IP**

## *Coleta de Informações*

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Figure 5 – Evidência - Porta ssh v. 7.4 (Aberta).

|  |  |  |
| --- | --- | --- |
| Portas | Serviços | Versão |
| 22 | OpenSSH | 7.4 |
| 65500 | OpenSSH | 7.4 |
| 3306 | MySQL | 5.7.23-enterprise-commercial-advanced-log |

## Vetores de Ataques Conhecidos

|  |
| --- |
| 65500/tcp open ssh OpenSSH 7.4 (protocol 2.0)  | vulners:  | cpe:/a:openbsd:openssh:7.4:  | EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 \*EXPLOIT\*  | EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 \*EXPLOIT\*  | EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 \*EXPLOIT\*  | EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 \*EXPLOIT\*  | CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111  | 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 \*EXPLOIT\*  | 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 \*EXPLOIT\*  | SSH\_ENUM 5.0 https://vulners.com/canvas/SSH\_ENUM \*EXPLOIT\*  | PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 \*EXPLOIT\*  | EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 \*EXPLOIT\*  | EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 \*EXPLOIT\*  | EDB-ID:45939 5.0 https://vulners.com/exploitdb/EDB-ID:45939 \*EXPLOIT\*  | EDB-ID:45233 5.0 https://vulners.com/exploitdb/EDB-ID:45233 \*EXPLOIT\*  | CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919  | CVE-2018-15473 5.0 https://vulners.com/cve/CVE-2018-15473  | CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906  | CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708  | 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 \*EXPLOIT\*  | CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617  | CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145  | CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110  | CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109  | CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685  | PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 \*EXPLOIT\*  | MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- \*EXPLOIT\*  |\_ 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 \*EXPLOIT\* |

Esta versão do OpenSSH há vários tipos de vulnerabilidades. É possível analisar vários vetores de ataque com essa versão.

## Possível correção

Atualização do serviço ssh para versão mais atual.

Atualização do sistema operacional para uma versão mais atual.

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 22 | OpenSSH | 7.4 |

## Vetores de Ataques Conhecidos

### Porta 22 - OpenSSH

|  |
| --- |
| 22/tcp open ssh OpenSSH 7.4 (protocol 2.0)  | vulners:  | cpe:/a:openbsd:openssh:7.4:  | EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 \*EXPLOIT\*  | EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 \*EXPLOIT\*  | EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 \*EXPLOIT\*  | EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 \*EXPLOIT\*  | CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111  | 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 \*EXPLOIT\*  | 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 \*EXPLOIT\*  | SSH\_ENUM 5.0 https://vulners.com/canvas/SSH\_ENUM \*EXPLOIT\*  | PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 \*EXPLOIT\*  | EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 \*EXPLOIT\*  | EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 \*EXPLOIT\*  | EDB-ID:45939 5.0 https://vulners.com/exploitdb/EDB-ID:45939 \*EXPLOIT\*  | EDB-ID:45233 5.0 https://vulners.com/exploitdb/EDB-ID:45233 \*EXPLOIT\*  | CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919  | CVE-2018-15473 5.0 https://vulners.com/cve/CVE-2018-15473  | CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906  | CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708  | 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 \*EXPLOIT\*  | CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617  | CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145  | CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110  | CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109  | CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685  | PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 \*EXPLOIT\*  | MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- 0.0 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH\_ENUMUSERS- \*EXPLOIT\*  |\_ 1337DAY-ID-30937 0.0 https://vulners.com/zdt/1337DAY-ID-30937 \*EXPLOIT\* |

Esta versão do OpenSSH há vários tipos de vulnerabilidades. É possível analisar vários vetores de ataque com essa versão.

## Possível correção

Atualização do serviço OpenSSH para a versão mais atual.

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 21 | ftp | - |
| 80 | http | - |
| 111 | rpcbind | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 443 | PRTG | - |
| 445 | microsoft-ds | - |
| 2049 | mountd | - |
| 3389 | ms-wbt-server | - |
| 5985 | - | - |
| 47001 | - | - |
| 49664 | msrpc | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49669 | msrpc | - |
| 49670 | msrpc | - |
| 49688 | msrpc | - |
| 49705 | msrpc | - |
| 49710 | msrpc | - |
| 49717 | msrpc | - |

## Vetores de Ataques Conhecidos

### Porta 443 - PRTG

|  |
| --- |
| 443/tcp open ssl/https PRTG  | ssl-dh-params:  | VULNERABLE:  | Diffie-Hellman Key Exchange Insufficient Group Strength  | State: VULNERABLE  | Transport Layer Security (TLS) services that use Diffie-Hellman groups  | of insufficient strength, especially those using one of a few commonly  | shared groups, may be susceptible to passive eavesdropping attacks.  | Check results:  | WEAK DH GROUP 1  | Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  | Modulus Type: Safe prime  | Modulus Source: Unknown/Custom-generated  | Modulus Length: 1024  | Generator Length: 8  | Public Key Length: 1024  | References:  |\_ https://weakdh.org  | http-slowloris-check:  | VULNERABLE:  | Slowloris DOS attack  | State: LIKELY VULNERABLE  | IDs: CVE:CVE-2007-6750  | Slowloris tries to keep many connections to the target web server open and hold  | them open as long as possible. It accomplishes this by opening connections to  | the target web server and sending a partial request. By doing so, it starves  | the http server's resources causing Denial Of Service.  |  | Disclosure date: 2009-09-17  | References:  | http://ha.ckers.org/slowloris/  |\_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 |

|  |
| --- |
| No exact OS matches for host (test conditions non-ideal).  TCP Sequence Prediction: Difficulty=17 (Good luck!)  IP ID Sequence Generation: Incrementing by 2  Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  Host script results:  | firewall-bypass:  |\_ Firewall vulnerable to bypass through ftp helper. (IPv4) |

Texto

Descrição gerada automaticamente

Figure - Evidência Firewall Bypass

### Logjam

A vulnerabilidade conhecida como "Logjam" que afeta a segurança de conexões com o protocolo HTTPS. A vulnerabilidade permite que um atacante intercepte e decifre conexões seguras, permitindo que eles acessem informações confidenciais.

A vulnerabilidade é causada por um problema com o modo como o protocolo Diffie-Hellman (DH) é implementado em muitos sistemas. O DH é um método criptográfico utilizado para estabelecer conexões seguras, permitindo que as partes troquem informações sem que um terceiro possa interceptar.

## Possível correção

Para proteger contra a vulnerabilidade Logjam, existem algumas medidas que podem ser tomadas:

Atualizar software: Certifique-se de que todos os sistemas e aplicativos estejam atualizados com as últimas correções de segurança. Isso inclui sistemas operacionais, servidores web, aplicativos cliente e outros softwares que usem o protocolo HTTPS.

Utilizar chaves fortes: Certifique-se de que suas chaves de segurança tenham pelo menos 2048 bits de tamanho. Isso ajuda a garantir que suas conexões sejam seguras mesmo se um atacante explorar a vulnerabilidade.

Utilizar criptografia DHE: Utilizar criptografia DHE (Diffie-Hellman Ephemeral) ao invés de DH (Diffie-Hellman) fixo. Isso ajuda a garantir que as conexões sejam seguras mesmo se um atacante explorar a vulnerabilidade.

Utilizar certificados de segurança válidos: Certifique-se de que seus certificados de segurança sejam válidos e emitidos por autoridades de certificação confiáveis. Isso ajuda a garantir que as conexões sejam seguras mesmo se um atacante explorar a vulnerabilidade.

Utilizar ferramentas de segurança: Utilize ferramentas de segurança, como firewalls, para proteger sua rede contra-ataques. Essas ferramentas podem ser configuradas para detectar e bloquear atividades maliciosas, como tentativas de explorar a vulnerabilidade Logjam.

Essas medidas podem ajudar a proteger sua rede contra a vulnerabilidade Logjam, mas é importante lembrar que a segurança é um processo contínuo e é importante manter-se atualizado e implementar medidas de segurança adicionais para manter seus sistemas protegidos.

## Slowloris DOS attack

A vulnerabilidade de segurança que afeta o protocolo ISAKMP (Internet Security Association and Key Management Protocol) usado para estabelecer conexões VPN (Virtual Private Network) seguras. A vulnerabilidade permite que um atacante intercepte e decifre pacotes de dados criptografados, permitindo que eles acessem informações confidenciais.

A vulnerabilidade é causada por um problema com a forma como o protocolo ISAKMP é implementado em alguns sistemas. Ele permite que um atacante intercepte e substitua pacotes de dados criptografados, permitindo que eles acessem informações confidenciais.

### Possível correção

Para se proteger dessa vulnerabilidade, é importante garantir que sistemas e software estejam atualizados com as últimas correções de segurança, e utilizar ferramentas de segurança para detectar e bloquear atividades maliciosas, como tentativas de explorar a vulnerabilidade.

## Bypass through ftp helper

A vulnerabilidade de "bypass through ftp helper" em um firewall significa que é possível contornar as restrições de segurança impostas pelo firewall utilizando o protocolo FTP (File Transfer Protocol). Isso pode permitir que usuários não autorizados acessem recursos e dados protegidos pelo firewall. Isso é geralmente causado por uma configuração inadequada do firewall ou uma falha de segurança no software do firewall.

### Possível correção

Configurar corretamente o firewall para bloquear o tráfego FTP: Isso pode ser feito configurando as regras de firewall para bloquear o tráfego FTP, ou desativando completamente a funcionalidade FTP no firewall.

Atualizar o software do firewall: As vulnerabilidades de segurança são frequentemente corrigidas em atualizações de software. Verifique se o seu firewall está executando a versão mais recente do software e instale qualquer atualização disponível.

Monitorar atividades de rede: Utilize ferramentas de monitoramento de rede para detectar atividades suspeitas, como tentativas de contornar as restrições de segurança do firewall.

Utilizar soluções de segurança avançadas: Utilize soluções de segurança avançadas, como firewalls de próxima geração ou soluções de segurança em nuvem, que oferecem maior proteção contra ameaças e vulnerabilidades.

Treinar os funcionários: É importante treinar os funcionários sobre boas práticas de segurança e sobre como evitar vulnerabilidades, incluindo a vulnerabilidade de "bypass through ftp helper"

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 3389 | ms-wbt-server | - |
| 5985 | http | - |
| 47001 | http | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49667 | msrpc | - |
| 49669 | msrpc | - |
| 49670 | msrpc | - |
| 49671 | msrpc | - |
| 49674 | msrpc | - |
| 49710 | msrpc | - |
| 49717 | msrpc | - |
| 49722 | msrpc | - |
| 56837 | msrpc | - |
| 63304 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 2179 | vmrdp | - |
| 3343 | ms-cluster-net | - |
| 3389 | ms-wbt-server | - |
| 5985 | http | - |
| 6160 | msrpc | - |
| 6162 | msrpc | - |
| 6163 | msrpc | - |
| 6190 | msrpc | - |
| 6290 | - | - |
| 6600 | mshvlm | - |
| 11731 | msrpc | - |
| 47001 | http | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49667 | msrpc | - |
| 49668 | msrpc | - |
| 49669 | msrpc | - |
| 49670 | msrpc | - |
| 49672 | msrpc | - |
| 49690 | msrpc | - |
| 49700 | msrpc | - |
| 51052 | msrpc | - |
| 55029 | msrpc | - |
| 55039 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 3389 | ms-wbt-server | - |
| 5985 | http | - |
| 47001 | http | - |
| 49664 | - | - |
| 49665 | - | - |
| 49666 | - | - |
| 49668 | - | - |
| 49669 | - | - |
| 49696 | msrpc | - |
| 49701 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 3389 | ms-wbt-server | - |
| 7070 | ssl/realserver | - |
| 47001 | http | - |
| 49664 | msrpc | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49668 | msrpc | - |
| 49682 | msrpc | - |
| 49696 | msrpc | - |
| 49702 | msrpc | - |
| 49708 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | - | - |
| 2179 | vmrdp | - |
| 3343 | ms-cluster-net | - |
| 3389 | ms-wbt-server | - |
| 5985 | http | - |
| 6600 | mshvlm | - |
| 47001 | http | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49667 | msrpc | - |
| 49668 | msrpc | - |
| 49669 | msrpc | - |
| 49670 | msrpc | - |
| 49671 | msrpc | - |
| 49674 | msrpc | - |
| 49722 | msrpc | - |
| 56775 | msrpc | - |
| 56837 | msrpc | - |
| 63304 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | Microsoft HTTPAPI httpd 2.0 |
| 111 | rpcbind | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 1063 | rpcbind | - |
| 2049 | rpcbind | - |
| 2179 | vmrdp | - |
| 3389 | ms-wbt-server | - |
| 5357 | http | Microsoft HTTPAPI httpd 2.0 |
| 5985 | http | Microsoft HTTPAPI httpd 2.0 |
| 6160 | ecmp | - |
| 6161 | msrpc |  |
| 6162 | msrpc | - |
| 6163 | pscribe | - |
| 6170 | storagecraft-image StorageCraft Image Manager | - |
| 6190 | - | - |
| 6290 | - | - |
| 6600 | mshvlm | - |
| 11731 | msrpc | - |
| 47001 | http | Microsoft HTTPAPI httpd 2.0 |
| 49664 | - | - |
| 49665 | - | - |
| 49666 | - | - |
| 49667 | - | - |
| 49668 | - | - |
| 49669 | - | - |
| 49671 | - | - |
| 49683 | - | - |
| 59993 | - | - |
| 64870 | - | - |

## Vetores de Ataques Conhecidos

### Porta 80 | 5357 | 5985

|  |
| --- |
| 80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |\_http-server-header: Microsoft-HTTPAPI/2.0  | http-slowloris-check:  | VULNERABLE:  | Slowloris DOS attack  | State: LIKELY VULNERABLE  | IDs: CVE:CVE-2007-6750  | Slowloris tries to keep many connections to the target web server open and hold  | them open as long as possible. It accomplishes this by opening connections to  | the target web server and sending a partial request. By doing so, it starves  | the http server's resources causing Denial Of Service.  |  | Disclosure date: 2009-09-17  | References:  | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  |\_ http://ha.ckers.org/slowloris/  |\_http-dombased-xss: Couldn't find any DOM based XSS.  |\_http-csrf: Couldn't find any CSRF vulnerabilities.  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  111/tcp open rpcbind  135/tcp open msrpc Microsoft Windows RPC  139/tcp open netbios-ssn Microsoft Windows netbios-ssn  445/tcp open microsoft-ds?  1063/tcp open rpcbind  2049/tcp open rpcbind  2179/tcp open vmrdp?  3389/tcp open ms-wbt-server Microsoft Terminal Services  5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |\_http-dombased-xss: Couldn't find any DOM based XSS.  | http-slowloris-check:  | VULNERABLE:  | Slowloris DOS attack  | State: LIKELY VULNERABLE  | IDs: CVE:CVE-2007-6750  | Slowloris tries to keep many connections to the target web server open and hold  | them open as long as possible. It accomplishes this by opening connections to  | the target web server and sending a partial request. By doing so, it starves  | the http server's resources causing Denial Of Service.  |  | Disclosure date: 2009-09-17  | References:  | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  |\_ http://ha.ckers.org/slowloris/  |\_http-csrf: Couldn't find any CSRF vulnerabilities.  |\_http-server-header: Microsoft-HTTPAPI/2.0  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  |\_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |\_http-server-header: Microsoft-HTTPAPI/2.0  | http-slowloris-check:  | VULNERABLE:  | Slowloris DOS attack  | State: LIKELY VULNERABLE  | IDs: CVE:CVE-2007-6750  | Slowloris tries to keep many connections to the target web server open and hold  | them open as long as possible. It accomplishes this by opening connections to  | the target web server and sending a partial request. By doing so, it starves  | the http server's resources causing Denial Of Service.  |  | Disclosure date: 2009-09-17  | References:  | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  |\_ http://ha.ckers.org/slowloris/  |\_http-dombased-xss: Couldn't find any DOM based XSS.  |\_http-csrf: Couldn't find any CSRF vulnerabilities.  |\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  |\_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug) |

## Slowloris DOS attack

A vulnerabilidade de segurança que afeta o protocolo ISAKMP (Internet Security Association and Key Management Protocol) usado para estabelecer conexões VPN (Virtual Private Network) seguras. A vulnerabilidade permite que um atacante intercepte e decifre pacotes de dados criptografados, permitindo que eles acessem informações confidenciais.

A vulnerabilidade é causada por um problema com a forma como o protocolo ISAKMP é implementado em alguns sistemas. Ele permite que um atacante intercepte e substitua pacotes de dados criptografados, permitindo que eles acessem informações confidenciais.

### Possível correção

Para se proteger dessa vulnerabilidade, é importante garantir que sistemas e software estejam atualizados com as últimas correções de segurança, e utilizar ferramentas de segurança para detectar e bloquear atividades maliciosas, como tentativas de explorar a vulnerabilidade.

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 80 | http | Microsoft HTTPAPI httpd 2.0 |
| 111 | rpcbind | - |
| 135 | msrcp | - |
| 139 | Netbios-ssn | - |
| 445 | microsoft-ds | - |
| 2049 | rpcbind | - |
| 2179 | vmrdp | - |
| 3389 | ms-wbt-server | - |
| 5357 | http | Microsoft HTTPAPI httpd 2.0 |
| 5985 | http | Microsoft HTTPAPI httpd 2.0 |
| 6160 | msrpc | - |
| 6161 | msrpc | - |
| 6163 | msrpc |  |
| 6170 | storagecraft-image | - |
| 6190 | storagecraft-image | - |
| 6290 | mshvlm | - |
| 6600 | msrpc | - |
| 11731 | msrpc | - |
| 47001 | http | Microsoft HTTPAPI httpd 2.0 |
| 49664 | msrpc | - |
| 49665 | msrpc | - |
| 49666 | msrpc | - |
| 49667 | msrpc | - |
| 49669 | msrpc | - |
| 49671 | msrpc | - |
| 49683 | msrpc | - |
| 64870 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 53 | domain | - |
| 135 | msrpc | - |
| 139 | netbios-ssn | - |
| 445 | microsoft-ds | - |
| 464 | kpasswd5 | - |
| 3260 | iscsi | - |
| 3389 | ms-wbt-server | - |
| 49666 | msrpc | - |
| 49667 | msrpc | - |
| 49670 | msrpc | - |
| 49675 | ncacn\_http | - |
| 49676 | msrpc | - |
| 49685 | msrpc |  |
| 49691 | msrpc | - |

## Vetores de Ataques Conhecidos

Não há possíveis vetores de ataques conhecidos.

## Possível correção

Fechar as portas desnecessárias

# **HOST IP**

## *Coleta de informações*

|  |  |  |
| --- | --- | --- |
| Portas Abertas | Serviços | Versão |
| 22 | OpenSSH | 7.9 |
| 53 | domain | - |
| 443 | ssl/http | - |
| 8080 | http-proxy | - |
| 8081 | blackice-icecap | - |

## Vetores de Ataques Conhecidos

### Porta 22 - OpenSSH

|  |
| --- |
| PORT STATE SERVICE VERSION  22/tcp open ssh OpenSSH 7.9 (protocol 2.0)  | vulners:  | cpe:/a:openbsd:openssh:7.9:  | EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 \*EXPLOIT\*  | EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 \*EXPLOIT\*  | EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 \*EXPLOIT\*  | EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 \*EXPLOIT\*  | CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111  | 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 \*EXPLOIT\*  | 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 \*EXPLOIT\*  | CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617  | CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905  | CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145  | CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110  | CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109  | CVE-2018-20685 2.6 https://vulners.com/cve/CVE-2018-20685  |\_ PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 \*EXPLOIT\* |

Esta versão do OpenSSH há vários tipos de vulnerabilidades. É possível analisar vários vetores de ataque com essa versão.

Ela permite que um atacante remoto sem autenticação execute comandos arbitrários no sistema alvo usando uma série de pacotes SSH maliciosos. Essa vulnerabilidade é causada por uma falha de verificação de tamanho incorreta no processamento de pacotes SSH e pode ser explorada por um atacante para obter acesso completo ao sistema alvo.

## Possível correção

Atualizar para a versão mais recente do OpenSSH: A versão 7.9p1 e superiores corrige essa vulnerabilidade, é recomendado que você faça a atualização o mais rápido possível.

Desabilitar o modo de roteamento de pacotes: Você pode desabilitar o modo de roteamento de pacotes no OpenSSH, impedindo que pacotes SSH maliciosos sejam processados pelo servidor.

Utilizar soluções de segurança avançadas: Utilize soluções de segurança avançadas, como firewalls de próxima geração ou soluções de segurança em nuvem, que oferecem maior proteção contra ameaças e vulnerabilidades.

Monitorar atividades de rede: Utilize ferramentas de monitoramento de rede para detectar atividades suspeitas, como tentativas de explorar essa vulnerabilidade.

**Conclusão da Análise Técnica**

|  |
| --- |
| **LIMPEZA DE RASTROS** |
| *Após a coleta das informações e evidências acima demonstradas, tudo que foi criado fora do contexto de produção foram devidamente excluídos.* |

# **Considerações Finais**

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios da empresa. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

Após a **EMPRESA** aplicar todas as correções sugeridas faremos um reteste nas vulnerabilidades apresentadas para comprovar que os problemas foram devidamente resolvidos.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Analista -

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gerente

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Líder Tecnologia da Informação

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gestor TI