TLP: CLEAR

BOLETIM DE SEGURANÇA

Vulnerabilidades no Rsync comprometem a segurança de servidores

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

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 INTRODUÇÃO EXECUTIVA

Recentemente, foram identificadas seis vulnerabilidades na ferramenta **Rsync**, amplamente utilizada para a sincronização de arquivos em servidores e sistemas Linux. As falhas apresentam diferentes níveis de gravidade, como crítica, permitindo a execução remota de código por atacantes não autenticados. Além disso, outras vulnerabilidades podem expor dados sensíveis e possibilitar a manipulação indevida de arquivos. Essas descobertas ressaltam riscos significativos para infraestruturas críticas, especialmente em sistemas de backup e replicação de dados, podendo impactar diversos setores.

Além disso, análises revelam que mais de **660.000 servidores Rsync** estão expostos globalmente, sendo 3.356 localizados no **Brasil**. Apesar de o número ser menor em relação a outros países, como China e Estados Unidos, esses servidores brasileiros continuam em risco elevado, especialmente se configurados com credenciais fracas ou acessos anônimos. Entre os servidores expostos globalmente, mais de 306.000 utilizam a porta TCP padrão 873, enquanto outros operam em portas alternativas, como a 8873, frequentemente usada para tunelamento SSH. Essa ampla exposição de servidores aumenta significativamente o risco de exploração, incluindo a possibilidade de ataques direcionados ao ambiente nacional. Diante disso, reforça-se a necessidade de ações imediatas, como a atualização para a versão 3.4.0 do Rsync e a implementação de medidas de segurança adicionais.

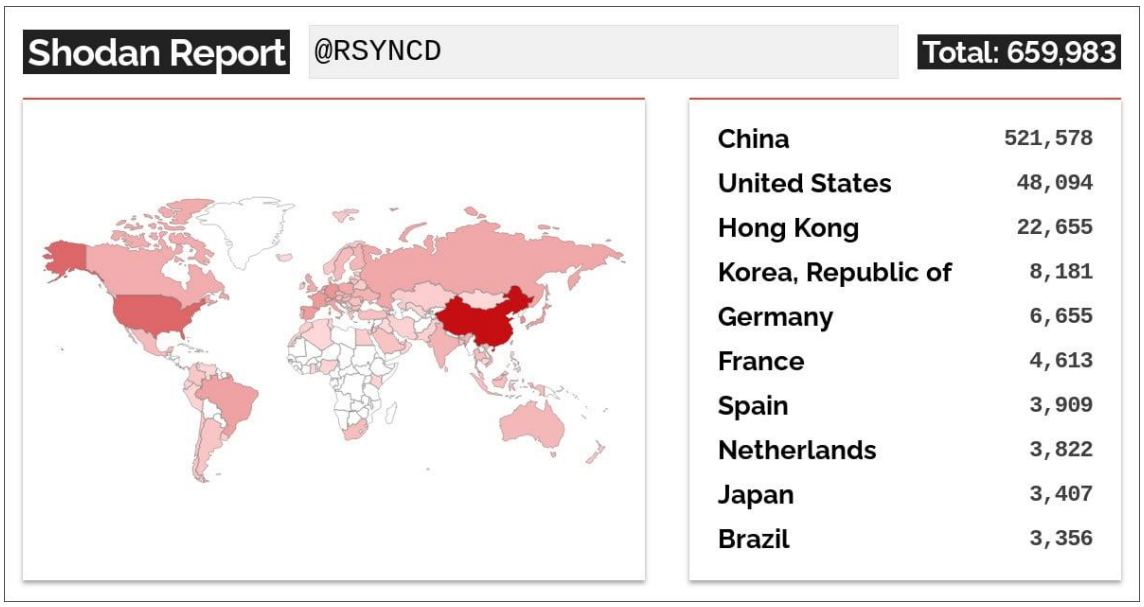

Figura 1 – Mapa Shodan de servidores Rsync expostos

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

As vulnerabilidades identificadas no Rsync afetam diversas versões **anteriores à 3.4.0** e exploram diferentes vetores, como execução remota de código, vazamento de informações e manipulação não autorizada de arquivos. Com impactos potenciais que incluem comprometimento de dados sensíveis, interrupções operacionais e movimentações laterais em redes corporativas, essas vulnerabilidades destacam a urgência de ações corretivas.

Para mitigar os riscos associados, foi lançada a **versão 3.4.0 do Rsync**, que corrige todas as falhas identificadas. A versão atualizada está disponível no repositório oficial de patches, como ilustrado na figura abaixo.

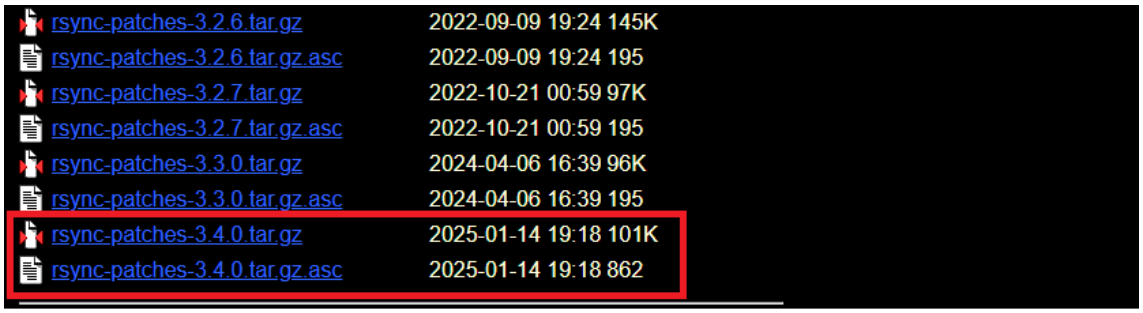

Figura 2 – Patches de atualização do Rsync 3.4.0.

Abaixo seguem as principais vulnerabilidades exploradas nas versões afetadas do Rsync, conforme relatado pelos pesquisadores:

- ***CVE-2024-12084*** *– Heap buffer overflow no Rsync, que permite a execução remota de código em servidores com acesso de leitura anônimo.*
- ***CVE-2024-12085*** *– Vazamento de informações da memória do processo (process memory disclosure) por meio de conteúdo de pilha não inicializado.*
- ***CVE-2024-12086*** *– Vulnerabilidade que permite que servidores Rsync maliciosos vazem arquivos arbitrários dos clientes conectados.*
- ***CVE-2024-12087*** *– Path traversal por meio da opção --inc-recursive, permitindo que um servidor remoto grave arquivos fora do diretório de destino.*
- ***CVE-2024-12088*** *– Path traversal explorando a opção --safe-links, que pode ser contornada para sobrescrever arquivos em diretórios não autorizados.*
- ***CVE-2024-12747*** *– Race condition durante a manipulação de links simbólicos, que pode ser usado para privilege escalation.*

Conforme já citado, estas vulnerabilidades podem ser exploradas tanto em servidores públicos de sincronização quanto em infraestruturas internas utilizadas para backups e replicação de dados. A exploração dessas falhas pode ser usada em ataques direcionados a redes corporativas, resultando em acesso não

autorizado, manipulação de arquivos críticos e roubo de informações confidenciais.

2.1 SISTEMAS AFETADOS

Abaixo segue os sistemas operacionais afetados pelas vulnerabilidades:

AlmaLinux OS Foundation	
Notificado: 25/11/2024 Atualizado:14/01/2025	
Data da declaração: 14 de janeiro de 2025	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado
CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Afetado

Arch Linux	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 02 de dezembro de 2024	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado
CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Desconhecido

Gentoo Linux	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 04 de dezembro de 2024	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado

CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Desconhecido

NixOS	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 14 de janeiro de 2025	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado
CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Afetado

Red Hat	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 14 de janeiro de 2025	
CVE-2024-12084	Não Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado
CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Afetado

Suse Linux	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 15 de janeiro de 2025	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado

CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Afetado

Triton Data Center	
Notificado: 25/11/2024 Atualizado: 14/01/2025	
Data da declaração: 07 de janeiro de 2025	
CVE-2024-12084	Afetado
CVE-2024-12085	Afetado
CVE-2024-12086	Afetado
CVE-2024-12087	Afetado
CVE-2024-12088	Afetado
CVE-2024-12747	Afetado

Tabela 1 – Status das vulnerabilidades CVE em fornecedores impactados.

2.2 IMPACTO DAS VULNERABILIDADES

A exploração das vulnerabilidades identificadas no Rsync pode resultar em diversos impactos, dependendo da falha explorada, incluindo:

- Comprometimento total de servidores através da execução remota de código (RCE).
- Vazamento de informações sensíveis por meio de disclosure de memória do processo.
- Manipulação não autorizada de arquivos críticos em sistemas vulneráveis.
- Movimentação lateral em redes corporativas, comprometendo outros sistemas conectados.
- Interrupção de processos essenciais, como backup e sincronização de dados.

3 RECOMENDAÇÕES

Atualizar para a versão Rsync 3.4.0

- Aplique imediatamente os patches de segurança disponibilizados na versão **Rsync 3.4.0**. Essa atualização corrige todas as seis vulnerabilidades conhecidas e deve ser priorizada para todos os sistemas que utilizam Rsync.

Evitar a exposição de servidores Rsync a redes não confiáveis

- Restrinja o acesso ao **daemon Rsync** apenas para endereços IP conhecidos e confiáveis. Evite expor servidores Rsync diretamente à Internet para minimizar o risco de exploração remota.

Desativar checksums vulneráveis

- Para mitigar as falhas relacionadas a checksums, compile o Rsync com as seguintes flags: **CFLAGS=-DDISABLE_SHA256_DIGEST** e **CFLAGS=-DDISABLE_SHA512_DIGEST**. Isso desabilita algoritmos vulneráveis e reduz o risco de exploração de heap buffer overflow.

Compilar o Rsync com proteção contra vazamento de memória

- Utilize a flag de compilação **-ftrivial-auto-var-init=zero** para zerar a memória não inicializada do processo. Essa medida reduz significativamente o risco de process memory disclosure (CVE-2024-12085).

Limitar o uso de recursos vulneráveis

- Desative ou limite o uso das opções **--inc-recursive** e **--safe-links** em configurações de servidores Rsync, especialmente quando o acesso é público. Essas opções estão diretamente ligadas a vulnerabilidades de path traversal e devem ser usadas com cautela.

Monitorar ferramentas que integram o Rsync

- Se sua organização utiliza ferramentas de backup que embutem o **Rsync**, como **Rclone** ou **ChronoSync**, verifique se essas ferramentas já aplicaram os patches mais recentes. Certifique-se de que todas as versões distribuídas estão atualizadas com a correção das vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NIST**
- **Red Hat**
- **CERT Coordination Center**
- **Shodan**
- **TheHackerNews**

5 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH