TLP: CLEAR

Pesquisa de WEB Exploitation

CVE-2019-5544: A reascensão de uma ameaça antiga

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1. INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência Heimdall da ISH Tecnologia, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: Estratégico, Tático e Operacional, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2. ESTRATÉGICO

As vulnerabilidades representam condições críticas que podem comprometer a disponibilidade, integridade e confidencialidade de ambientes corporativos. Nesta seção, destacamos a CVE-2019-5544, uma falha de segurança com relevância estratégica devido à sua gravidade e alto índice de exploração ativa no Brasil.

2.1 INTRODUÇÃO SOBRE A VULNERABILIDADE

A **CVE-2019-5544** refere-se a uma falha crítica **(CVSSv3 de 9.8)** de segurança em **OpenSLP**, componente utilizado em ambientes **VMware ESXi** e *appliances* **Horizon DaaS**. A vulnerabilidade consiste em uma condição de ***heap overwrite***, que pode ser explorada remotamente para execução de código sem necessitar autenticação. Com acesso à **porta de rede 427** (usada por **OpenSLP**) os atores de ameaça podem abusar dessa vulnerabilidade para executar comandos arbitrários no sistema alvo.

Além de sua gravidade intrínseca, a vulnerabilidade segue apresentando **alta taxa de exploração ativa no Brasil**. Dados coletados pelo *Shadowserver* indicam que, no último mês, a **CVE-2019-5544** esteve entre as vulnerabilidades mais exploradas em alvos expostos à internet no país, com destaque no diagrama abaixo:

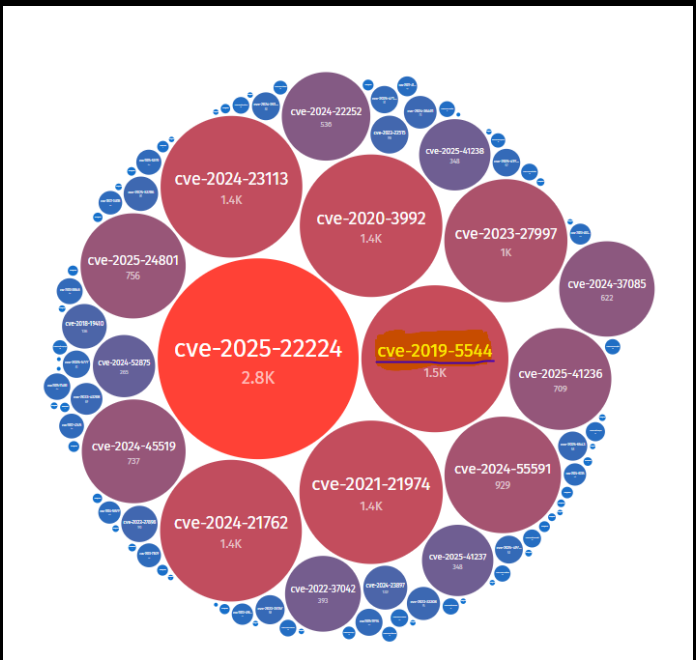

Figura 1 - Incidência da CVE-2019-5544 no Brasil

Na imagem abaixo temos o **EPSS** (***Exploit Prediction Scoring System***), no qual demonstra que a **CVE-2019-5544** apresentava até 2024 uma baixa probabilidade de exploração prática, variando entre 3% e 20%. Contudo, em 2025 podemos observar um aumento expressivo, com pontuação superior a **85%**, o que indica uma probabilidade significativamente maior de exploração ativa por atores de ameaça.

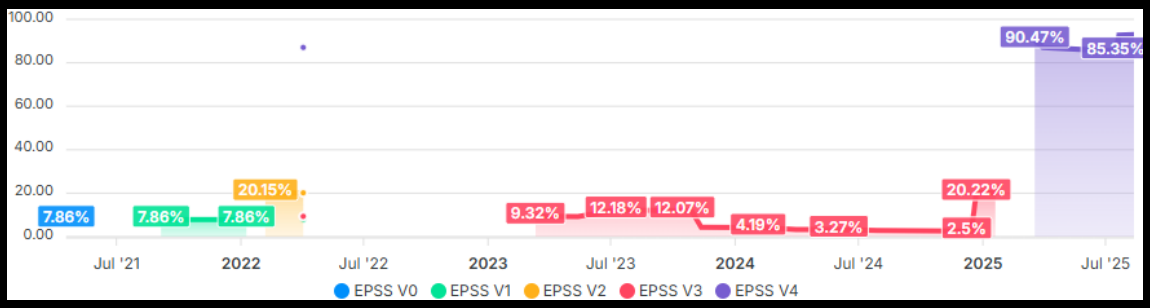

Figura 2 - EPSS CVE-2019-5544

Essa evolução evidencia que vulnerabilidades "antigas" podem ganhar relevância repentina, seja pela divulgação de *exploits* públicos, integração em *kits* de ataque ou pelo crescimento de campanhas que visam sistemas legados ainda em operação.

2.2 Sistemas, Segmentos e Produtos afetados

Produtos afetados e versões:

- **VMware ESXi**, versões 6.0, 6.5 e 6.7 (ambas com atualizações específicas) *Support Portal*.
- **Horizon DaaS Virtual Appliance**, versões até a 8.x *Support Portal*.

Componentes afetados:

- Implementações de **OpenSLP (*Service Location Protocol*)** dentro dos produtos citados, até a versão afetada cvedetails.comdatacipher.com.

Contexto e segmentos impactados:

- **Ambientes de virtualização**, como data centers e provedores de nuvem que executam *VMware* **ESXi**, ficam diretamente expostos ao risco de exploração remota.
- **Infraestruturas críticas corporativas**, frequentemente baseadas em ***VMware*** para hospedagem de máquinas virtuais, são extremamente vulneráveis a ataques que podem comprometer múltiplas VMs e serviços.
- Como reportado por órgãos como CISA, essa vulnerabilidade já foi vista como utilizada em campanhas de *ransomware*, ampliando o risco para ambientes de produção.

VMWARE | VMWARE ESXI AND HORIZON DAAS

CVE-2019-5544

VMware ESXi and Horizon DaaS OpenSLP Heap-Based Buffer Overflow Vulnerability: *VMware ESXi and Horizon Desktop as a Service (DaaS) OpenSLP contains a heap-based buffer overflow vulnerability that allows an attacker with network access to port 427 to overwrite the heap of the OpenSLP service to perform remote code execution.*

Related CWE: CWE-787

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply updates per vendor instructions.

- **Date Added:** 2021-11-03
- **Due Date:** 2022-05-03

Figura 3 -Vulnerabilidade no catalogo KEV-CISA

Contexto e segmentos impactados:

Além dos produtos e segmentos listados, a distribuição geográfica dos ativos vulneráveis evidencia que o **Brasil está entre os países com maior presença de sistemas potencialmente expostos**, conforme ilustrado na imagem abaixo:

Figura 4 - Mapa de calor com destaque dos países com maior exposição

A imagem evidencia uma maior exposição do Brasil à exploração da CVE-2019-5544, o que reforça a urgência da adoção de medidas de mitigação e aplicação de patches pelas organizações nacionais.

3. TÁTICO

3.1 USO DA CVE-2019-5544 EM CAMPANHAS

A **CVE-2019-5544** tem sido explorada por diferentes grupos de *ransomware*, resultando na criptografia em massa de máquinas virtuais.

Exemplos documentados:

- **RansomExx / Defray777** – Observado explorando a CVE-2019-5544 em conjunto com a **CVE-2020-3992** para obter acesso inicial a *hosts* ESXi e implantar cargas de *ransomware*.
- **DarkSide /BlackMatter** – Grupos afiliados utilizaram falhas em serviços *VMware* expostos para garantir persistência em ambientes de virtualização, mirando na rápida criptografia de múltiplas VMs de uma só vez.
- **LockBit** – *Leaks* e investigações indicam que operadores procuram ativamente ESXi vulneráveis (incluindo exposição da porta 427/SLP) como forma de entrada privilegiada para implantações massivas de *ransomware*.
- **ESXiArgs** – Embora não diretamente ligado apenas à CVE-2019-5544, campanhas de larga escala contra ESXi destacaram a relevância do vetor SLP e a exploração de falhas não corrigidas em *hypervisors VMware*.

3.2 CONDIÇÕES PARA A EXPLORAÇÃO DA VULNERABILIDADE

A exploração da CVE-2019-5544 para cada grupo APT, pode desempenhar um papel diferente dentro da **cadeia de ataque**, abaixo destacamos algumas dessas técnicas/vetores, mapeados segundo os atores de ameaça citados anteriormente:

MITRE ATT&CK ID	Descrição	Grupos observados
Initial Access (T1190 – Exploit Public-Facing Application)	Exploração remota via SLP (porta 427) para execução de código sem autenticação.	RansomExx, LockBit
Execution (T1059 – Command and Scripting Interpreter)	Implantação de scripts ou binários maliciosos após a execução remota de código.	ESXiArgs
Privilege Escalation (T1068 – Exploitation for Privilege Escalation)	Uso combinado de falhas adicionais (ex: CVE-2020-3992) para ampliar privilégios no host.	RansomExx
Impact (T1486 – Data Encrypted for Impact)	Criptografia massiva de VMs no ESXi comprometido.	DarkSide, LockBit

Tabela 1 - Mitre ID x Campanha

4. OPERACIONAL

4.1 POSSIBILIDADE DE DETEÇÃO

A exploração da CVE-2019-5544 pode ser identificada a partir de:

- **Monitoramento de rede**: inspeção de tráfego anômalo direcionado à porta **427/UDP**, utilizada pelo SLP;
- **Análise de logs do ESXi**: verificação de mensagens de erro ou chamadas incomuns ao serviço slpd;
- **Telemetria de segurança (NDR/IDS/IPS)**: regras para detecção de exploração SLP conhecidas (Snort/Suricata);
- **Atividade pós-exploração**: correlação com criação inesperada de processos, modificação de arquivos de configuração do ESXi ou disparo de operações administrativas fora de rotina.

Condição	Descrição
Porta/Protocolo	**UDP/427** exposto a redes externas
Processo	Atividade anômala associada ao **slpd**
Assinatura IDS/IPS	Exploração de buffer overflow em SLP (**ServiceRequest**)
Indicadores comportamentais	Conexões não usuais seguidas de execução de comandos administrativos

Tabela 2 - Indicadores viáveis para detecção

4.2 MITIGAÇÃO

A mitigação deve priorizar a redução de exposição do SLP e aplicação de correções.

Correção imediata

- Aplicar os patches de segurança da *VMware* que corrigem a CVE-2019-5544;
- Encerrar o serviço slpd em hosts ESXi onde não seja estritamente necessário.

Mitigação temporária

- Restringir acesso à porta **427/UDP** via firewall, permitindo apenas comunicação interna controlada;
- Implementar segmentação de rede para isolar *hosts* de virtualização críticos;
- Aplicar regras emergenciais em WAF/IDS/IPS para bloquear pacotes SLP malformados.

Ações defensivas adicionais

- Monitorar continuamente a superfície de ataque para evitar exposição inadvertida da porta 427;
- Incluir validações de segurança em processos de *hardening* de ESXi;
- Integrar alertas em SIEM para correlação de tentativas de exploração com movimentação lateral ou execução de *ransomware*.

5. CONCLUSÃO

A exploração da CVE-2019-5544 evidência como falhas consideradas **“antigas”** podem manter impacto significativo em cenários atuais, transformando-se em vetores críticos para campanhas de *ransomware*. O fato de grupos distintos de ***RansomExx*** a ***LockBit***, continuarem explorando a vulnerabilidade reforça sua relevância no ecossistema de ameaças e confirma a atratividade de ambientes de virtualização. Do ponto de vista defensivo, a principal recomendação é **reduzir a superfície de ataque**: desabilitar o SLP sempre que possível, manter *hosts* atualizados e aplicar segmentação de rede. Em paralelo, mecanismos de detecção e resposta devem monitorar tanto tentativas de exploração da porta 427/UDP quanto atividades pós-comprometimento, permitindo contenção rápida antes da execução massiva de *ransomware*.

Outro ponto crítico é o impacto regional: levantamentos recentes apontam o **Brasil entre os países com maior exposição à CVE-2019-5544**, indicando não apenas a permanência de *hosts VMware* desatualizados acessíveis na internet, mas também uma janela de exploração ativa que vem sendo aproveitada por diferentes atores. A CVE-2019-5544, portanto, não deve ser vista como uma vulnerabilidade pontual, mas como parte de cadeias de ataque mais amplas. Sua exploração recorrente destaca a importância de uma abordagem contínua de **gestão de vulnerabilidades, monitoramento proativo e correlação de eventos**, alinhada às práticas de *hardening* em ambientes de virtualização críticos.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- MITRE ATT&CK
- NIST
- CVEFIND
- CVEDETAILS
- SHADOWSERVER
- CISA-KEV

AUTORES

Gustavo Jatene de oliveira – Threat Researcher

heimdall
security research
A DIVISION OF ISH