Your IT Company

Principais Vulnerabilidades e Ameaças (Julho/24)

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Um novo RaaS (ransomware-as-a-service) nomeado como Eldorado vem atacando hosts com Windows e máquinas virtuais VMware ESXi 2
2.2. Encontrada vulnerabilidade zero-day de escalação de privilégio zero-day no Windows Hyper-V 7
2.3. RegreSSHion, vulnerabilidade recém-descoberta permite execução remota de código não autenticado no servidor OpenSSH 8
2.4. Recente vulnerabilidade no protocolo RADIUS, torna redes expostas a ataque man-in-the-middle . 11

1. Objetivo

Este documento foi desenvolvido e fundamentado utilizando as documentações oficiais do NIST (National Institute Of Standards and Technology), MITRE e CVE.org, que são conhecidas mundialmente na área de cibersegurança, como modelo e padronização de melhores práticas de segurança, pesquisa de metodologias de ataques e defesa cibernética, e pesquisa e catalogação de novas vulnerabilidades em sistemas operacionais e aplicações.

Para ver mais sobre vulnerabilidades acesse o endereço interno: https://servicesecurity.sharepoint.com/:u:/r/sites/ComitEditorial/SitePages/Vulnerabilidades-(CVEs).aspx?csf=1&web=1&share=EfmfMqeKLR1Nin36yYlXeOsBT8dah8so1vtwJOkTa0omKg&e=hv0atg.

2. Vulnerabilidades e Ameaças descobertas

2.1. Um novo RaaS (ransomware-as-a-service) nomeado como Eldorado vem atacando hosts com Windows e máquinas virtuais VMware ESXi

Programas de parceria para cibercriminosos, também conhecidos como Ransomware-as-a-Service (RaaS), evoluíram para operações sofisticadas que se assemelham a grandes empresas. Esses programas de parceria recrutam afiliados para executar papéis específicos em redes cibercriminosas, com foco particular na entrega e execução de ataques de ransomware em empresas. Ao longo dos anos, o processo de seleção para afiliados mudou de um foco na experiência individual e acesso à rede para uma abordagem mais sistemática.

Entre 2022 e 2023, analistas identificaram 27 anúncios de programas de RaaS em fóruns da dark web. Esses anúncios mencionavam tanto programas bem conhecidos, como Yanluowang, Qilin, Knight e qBit, quanto ferramentas menos conhecidas que ainda não foram observadas em ataques reais. Em 2023, o número de anúncios publicados em fóruns da dark web em busca de parceiros para programas de RaaS aumentou 1,5 vezes em comparação com 2022, destacando a crescente demanda por afiliados qualificados.

Ao analisar os novos programas de afiliados, os analistas encontraram um novo anúncio no fórum da dark web sobre a busca por pentesters para se juntar à equipe de um novo locker.

Em março de 2024, um anúncio para um novo programa de afiliados foi postado no fórum de ransomware “RAMP”. O post anunciava a disponibilidade de um locker e loader, enquanto buscava pentesters para se juntar à equipe. Pesquisadores infiltraram-se no grupo Eldorado e descobriram que o representante do grupo era um falante de russo. O construtor do ransomware solicitou a senha do administrador de domínio ou o hash NTLM (Windows New Technology LAN Manager) e outros parâmetros para gerar amostras de ransomware.

O Eldorado possui duas versões do malware em seu arsenal para Windows e Linux. No entanto, este desenvolvimento é único e não depende de fontes de construtores previamente publicadas. Por exemplo, em 21 de setembro de 2022, o construtor do ransomware LockBit 3.0 foi vazado, permitindo que vários atores de ameaças criassem suas próprias versões e conduzissem numerosos ataques de alto perfil usando suas técnicas robustas de criptografia e evasão. Da mesma forma, o código-fonte do ransomware Babuk foi vazado em 1º de setembro de 2021, levando à criação de várias cepas de ransomware por diferentes grupos para explorar e exfiltrar dados de redes alvo. Exemplos notáveis incluem o grupo de ransomware LIMPOPO (também conhecido como SOCOTRA, FORMOSA, SEXi), o ransomware BabLock e o ransomware Estate.

Classificação: Público

O ransomware Eldorado usa Golang para capacidades multiplataforma, empregando Chacha20 para criptografia de arquivos e Rivest Shamir Adleman-Optimal Asymmetric Encryption Padding (RSA-OAEP) para criptografia de chaves. Ele pode criptografar arquivos em redes compartilhadas usando o protocolo Server Message Block (SMB). Parâmetros-chave para personalização durante a construção incluem redes alvo ou nomes de empresas, detalhes da nota de resgate e credenciais de administrador.

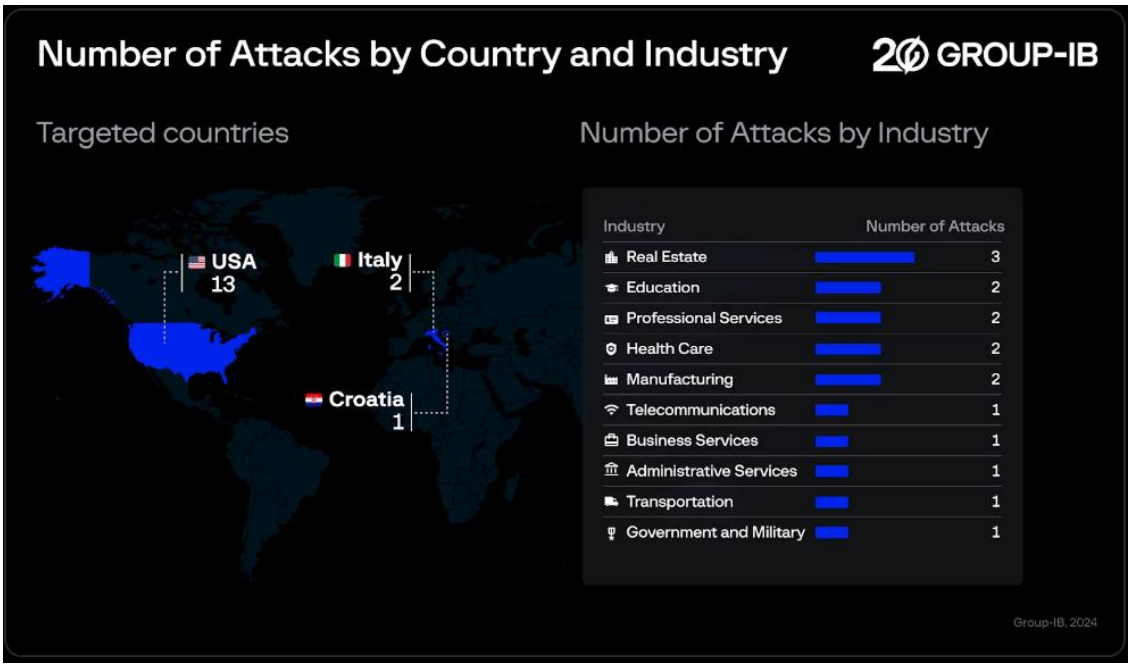

Figura 1 - Número de ataques utilizando o Eldourado por pais e segmentos de empresas. Fonte: https://www.group-ib.com/blog/eldorado-ransomware/

Exploração

Durante a análise do criptografador, os analistas descobriram que o ransomware Eldorado é escrito em Golang. Existem versões do Eldorado para Windows (32 bits e 64 bits) e Linux (32 bits e 64 bits). A escolha do uso da linguagem de programação Go pode ser devido às suas capacidades multiplataforma. A capacidade dos programas Go de cross-compilar código em binários nativos e autossuficientes pode ser uma razão pela qual os autores de malware preferiram desenvolver em Golang.

Todos os arquivos criptografados terão a extensão ".00000001". Durante o processo de bloqueio, os seguintes logs são impressos no console podem ser visualizados abaixo.

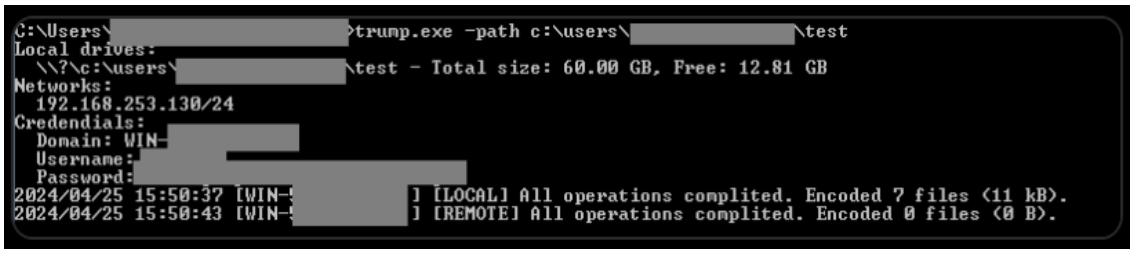

Figura 2 – Logs do console durante a encriptação. Fonte: https://www.group-ib.com/blog/eldorado-ransomware/

Classificação: Público

Uma nota de resgate intitulada “HOW_RETURN_YOUR_DATA.TXT” será escrita nas pastas Documentos e Desktop, contendo instruções para contatar o TA. O nome do arquivo e o texto da nota de resgate podem ser personalizados durante o processo de construção.

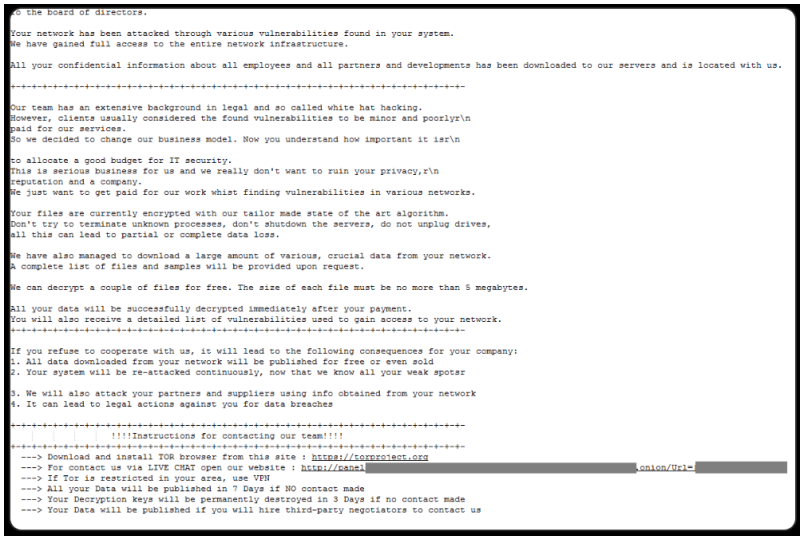

Figura 3 - Nota de resgate com URL para acessar um chat ao vivo com os atacantes. Fonte: https://www.group-ib.com/blog/eldorado-ransomware/

Exploração Windows

A versão do Eldorado ransomware para Windows aceita vários parâmetros de linha de comando. A tabela abaixo lista as opções disponíveis, juntamente com suas descrições correspondentes:

Argumentos	Descrição
path	Criptografa todos os arquivos no diretório fornecido (e seus subdiretórios); sem ele, os discos locais serão processados.
-skip-local	Pula o processamento de arquivos locais.
-n <subnet>	Compartilhamentos no formato CIDR, por exemplo, 10.0.1.0/24. Se não especificado, valores das interfaces de rede ativas serão usados. Também pode ser especificado um arquivo com uma lista de redes.
-d <domain>	Especifica um domínio.
-u <username>	Especifica o nome de usuário para SMB.
-p <password>	Especifica a senha para SMB.
-skip-net	Pula o processamento de compartilhamentos.
-keep	Desabilita a autodeleção após a execução; por padrão, o executável se autodeleta.

Dentro do binário, há um blob de configuração comprimido em gzip. A configuração contém os seguintes campos:

```
type main.EC struct {
    K  []uint8  // chave pública
    NN string   // nome da nota
    NT []uint8  // texto da nota
```


Classificação: Público

```
DA string   // senha ou hash do admin do domínio
}
```

Na amostra que analisamos, encontramos que alguns logs são enviados para 173.44.141[.]152 via websockets com o cabeçalho Origin definido como “http://logger”.

Quando fornecido com as credenciais de usuário apropriadas, ele pode criptografar arquivos em redes compartilhadas. Ele utiliza o protocolo SMB e depende da biblioteca cliente SMB2/3 para essa funcionalidade.

O ransomware Eldorado usa Chacha20 para criptografar arquivos e RSA-OAEP para criptografar a chave gerada.

Para cada arquivo, ele gerará uma chave de 32 bytes e um nonce de 12 bytes, e criptografará o arquivo usando Chacha20. A chave e o nonce serão criptografados com RSA-OAEP com a chave pública embutida da configuração e anexados ao final de cada arquivo.

Para remover quaisquer vestígios, o ransomware Eldorado executa um comando PowerShell para sobrescrever o criptografador com bytes aleatórios antes de excluir o arquivo. Essa ação não será realizada se “-keep” for especificado nos argumentos do comando.

```
$f=;
while(Test-Path -Path $f)
{
$o=new-object byte[] 10485760;
(new-object Random).NextBytes($o);
[IO.File]::WriteAllBytes($f,$o);
Remove-Item -Path $f;
Sleep 1;
}
```

Em seguida, remove as cópias de volume de sombra no final da execução. Cópias de volume de sombra são um mecanismo de backup usado no Windows que pode ser usado para recuperar arquivos se forem perdidos ou danificados, e é executado através do seguinte comando:

```
vssadmin delete shadows /all /quiet
```

Durante a análise do comportamento do ransomware Eldorado, foi observado que ele exclui determinados diretórios, arquivos e extensões de arquivo de sua criptografia. Aqui estão as exclusões específicas:

Diretórios excluídos	Arquivos excluídos	Extensões de Arquivo Excluídas
C:\Windows	ntldr	.00000001
C:\ProgramData	ntdetect.com	.exe
C:\Program Files	autoexec.bat	.dll
C:\Program Files (x86)	ntuser.dat	.sys
C:$Recycle.Bin	ntuser.dat.log	.msi
C:\Users\All Users	iconcache.db	.ini
C:\WinNT	bootsect.bak	.inf

Classificação: Público

C:\Users[usuário]\AppData	bootfont.bin	.lnk
C:\Users[usuário]\Application Data	bootmgr	.00000001
C:\Users[usuário]\Local Settings	thumbs.db	.exe

Exploração Linux

Para o Linux, o criptografador do ransomware Eldorado é mais simples e suporta apenas o argumento -path. Ele percorrerá recursivamente os arquivos no diretório especificado. O algoritmo de criptografia permanece o mesmo da versão para Windows.

Mitigação e Prevenção

Embora os grupos de ransomware tenham ganhado notoriedade por atacar empresas em setores críticos, eles são uma ameaça para organizações de todos os setores. Além de terem novos membros em sua rede, os programas de afiliados de ransomware equipam os membros com ferramentas e técnicas aprimoradas. Dito isso, é essencial que as empresas tomem medidas específicas imediatamente para manter suas operações críticas e dados seguros. A seguir as melhores recomendações:

- **Adicione mais camadas de segurança:** Soluções de autenticação multifator (MFA) e acesso baseado em credenciais.
- **Pare o ransomware com detecção precoce:** Utilize as capacidades de detecção comportamental da solução de Endpoint Detection and Response (EDR) para ajudar a identificar indicadores de ransomware em seus endpoints gerenciados.
- **Tenha uma estratégia de backup:** Os processos de backup de dados devem ser realizados regularmente, pois reduzem os danos e ajudam as organizações a evitar a perda de dados após ataques de ransomware.
- **Aplique patches regularmente:** Quanto mais tempo uma vulnerabilidade permanecer sem correção, maior o risco de ser explorada por cibercriminosos. Os patches de segurança devem, portanto, ser priorizados, e as organizações também devem estabelecer um processo para revisar e aplicar patches regularmente à medida que estiverem disponíveis.
- **Treine os funcionários:** O fator humano continua sendo uma das maiores vulnerabilidades na cibersegurança. Eduque os funcionários sobre os riscos relacionados à rede, ativos, dispositivos e infraestrutura da organização.
- **Controle vulnerabilidades:** Não ignore vulnerabilidades emergentes. Verificar sua infraestrutura anualmente com uma auditoria técnica ou avaliação de segurança não é apenas um bom hábito, mas também adiciona uma camada de proteção necessária.
- **Nunca pague o resgate:** Em 97% dos ataques de ransomware, é impossível recuperar o acesso aos dados sem o software de descriptografia.

Além disso é recomendado adicionar as seguintes IOCs a lista de bloqueios (não esqueça de substituir o hxxp por http e remover os []):

IOCs	Descrição
1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b	Hash – SHA256 Eldorado (32-bit windows)

Classificação: Público

7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd	Hash – SHA256 Eldorado (64-bit windows)
cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7	Hash – SHA256 Eldorado (64-bit windows)
b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de	Hash – SHA256 Eldorado (32-bit linux)
dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33	Hash – SHA256 Eldorado (64-bit linux)
173.44.141[.]152	Endereço IP

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.group-ib.com/blog/eldorado-ransomware/ e https://www.bleepingcomputer.com/news/security/new-eldorado-ransomware-targets-windows-vmware-esxi-vms/

2.2. Encontrada vulnerabilidade zero-day de escalação de privilégio zero-day no Windows Hyper-V

O Windows Hyper-V permite a virtualização de hardware. Profissionais de TI e desenvolvedores de software usam a virtualização para testar software em vários sistemas operacionais. O Hyper-V permite que profissionais realizem essas tarefas de forma eficiente. Com a ajuda do Hyper-V, é possível criar discos rígidos virtuais, switches virtuais e diversos dispositivos virtuais diferentes, todos os quais podem ser adicionados a máquinas virtuais.

Recentemente foi encontrada uma vulnerabilidade zero-day no Windows Hyper-V que permite a escalação de privilégios

A vulnerabilidade recebeu a identificação: CVE-2024-38080 que foi classificada de acordo com o NIST com a pontuação CVSS v3.1: 7.8 de nível alto. E está descrita como: “Vulnerabilidade de escalação de privilégios no Windows Hyper-V”.

Esta vulnerabilidade permite que um atacante eleve seus privilégios a nível de administrador no sistema host. Esta vulnerabilidade ocorre devido a uma falha na validação de entradas no serviço Hyper-V, que pode ser explorada para executar código arbitrário com privilégios elevados.

Exploração

Para explorar essa vulnerabilidade, um atacante precisa ter acesso ao sistema guest do Hyper-V. A exploração típica envolve:

Injeção de Código Malicioso: O atacante injeta código malicioso no sistema guest, aproveitando a falha de validação de entradas do Hyper-V.

Escalação de Privilégio: O código malicioso é executado no contexto do Hyper-V, permitindo ao atacante elevar seus privilégios e obter controle total sobre o sistema host.

Persistência: Uma vez que o controle é estabelecido, o atacante pode instalar backdoors e outras ferramentas maliciosas para manter acesso contínuo e indetectável.

Mitigação

Para mitigar a CVE-2024-38080, recomenda-se a implementação das seguintes medidas:

- Aplicação de Patches: A Microsoft lançou um patch de segurança para corrigir essa vulnerabilidade. Certifique-se de que todos os sistemas Hyper-V estão atualizados com as últimas correções disponíveis.

Classificação: Público

- Qualys VMDR: Utilize o Qualys VMDR para identificar e priorizar a aplicação de patches nos sistemas afetados.

  Consulta de Vulnerabilidade: vulnerabilities.vulnerability.qid:92024
- Configurações de Segurança: Reforce as configurações de segurança do Hyper-V, limitando o acesso ao sistema guest apenas a usuários autorizados e monitorando atividades suspeitas.
- Trend Micro Vision One: Configure políticas de monitoramento para detectar e bloquear atividades anômalas no Hyper-V.
- Monitoramento Contínuo: Implemente soluções de monitoramento contínuo para identificar tentativas de exploração da vulnerabilidade e outras atividades suspeitas.
- Qualys Continuous Monitoring: Configure alertas em tempo real para detectar qualquer tentativa de exploração.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2024-38080 e https://blog.qualys.com/vulnerabilities-threat-research/2024/07/09/microsoft-patch-tuesday-july-2024-security-update-review

2.3. RegreSSHion, vulnerabilidade recém-descoberta permite execução remota de código não autenticado no servidor OpenSSH

A Qualys Threat Research Unit descobriu uma vulnerabilidade de RCE (Remote Unauthenticated Code Execution) no servidor OpenSSH (sshd) em sistemas Linux baseados em glibc. O CVE atribuído a esta vulnerabilidade é CVE-2024-6387.

A vulnerabilidade (CVE-2024-6387) está classificada de acordo com o NIST com pontuação CVSS v3.1: 8.1 de nível alto e está descrita: “Uma regressão de segurança foi descoberta no servidor do OpenSSH (sshd). Há uma condição de corrida que pode levar o sshd a manipular alguns sinais de forma insegura. Um invasor remoto não autenticado pode ser capaz de acioná-la ao falhar na autenticação dentro de um período definido”.

Com base em pesquisas realizadas foram identificados mais de 14 milhões de instâncias de servidores OpenSSH potencialmente vulneráveis expostas à Internet. Dados anonimizados do Qualys CSAM 3.0, combinados com informações do External Attack Surface Management, revelam que aproximadamente 700.000 dessas instâncias estão vulneráveis. Isso representa 31% de todas as instâncias OpenSSH voltadas para a Internet localizada na base global de clientes da Qualys. Notavelmente, mais de 0,14% dessas instâncias vulneráveis estão executando uma versão de fim de vida ou fim de suporte do OpenSSH.

Exploração

Essa vulnerabilidade, se explorada, pode levar ao comprometimento total do sistema, permitindo que um invasor execute código arbitrário com os privilégios mais altos. Isso resultaria na aquisição completa do sistema, instalação de malware, manipulação de dados e criação de backdoors para acesso persistente. Tal situação facilitaria a propagação na rede, permitindo que os invasores usassem um sistema comprometido como ponto de apoio para explorar outros sistemas vulneráveis dentro da organização.

Classificação: Público

Além disso, obter acesso root permitiria que os invasores contornassem mecanismos críticos de segurança, como firewalls, sistemas de detecção de intrusão e mecanismos de registro, obscurecendo ainda mais suas atividades. Isso também poderia resultar em violações e vazamentos de dados significativos, dando aos invasores acesso a todos os dados armazenados no sistema, incluindo informações confidenciais ou proprietárias que poderiam ser roubadas ou divulgadas publicamente.

Essa vulnerabilidade é difícil de explorar devido à sua natureza de condição de corrida remota, exigindo várias tentativas para um ataque bem-sucedido. Isso pode causar corrupção de memória e exigir a superação do ASLR (Address Space Layout Randomization). Os avanços no aprendizado profundo podem aumentar significativamente a taxa de exploração, potencialmente fornecendo aos invasores uma vantagem substancial no aproveitamento de tais falhas de segurança.

Versões afetadas do OpenSSH:

- As versões do OpenSSH anteriores à 4.4p1 são vulneráveis a essa condição de corrida do manipulador de sinal, a menos que sejam corrigidas para CVE-2006-5051 e CVE-2008-4109.
- Versões de 4.4p1 até, mas não incluindo, 8.5p1 não são vulneráveis devido a um patch transformador para CVE-2006-5051, que tornou uma função anteriormente insegura segura.
- A vulnerabilidade ressurge em versões de 8.5p1 até, mas não incluindo, 9.8p1 devido à remoção acidental de um componente crítico em uma função.
- Os sistemas OpenBSD não são afetados por esse bug, pois o OpenBSD desenvolveu um mecanismo seguro em 2001 que previne essa vulnerabilidade.

Mitigação e Prevenção com Qualys

A vulnerabilidade regreSSHion no OpenSSH, exige uma abordagem de segurança focada em camadas. A seguir constam recomendações estratégicas para as empresas se protegerem contra essa ameaça significativa:

- Gerenciamento de patches: Aplique rapidamente os patches disponíveis para o OpenSSH e priorize os processos de atualização em andamento.
- Controle de acesso aprimorado: Limite o acesso SSH por meio de controles baseados em rede para minimizar os riscos de ataque.
- Segmentação de rede e detecção de intrusão: Divida as redes para restringir o acesso não autorizado e os movimentos laterais em ambientes críticos. Implante sistemas para monitorar e alertar sobre atividades incomuns indicativas de tentativas de exploração.

Descoberta de ativos vulneráveis usando o Qualys CyberSecurity Asset Management (CSAM):

A etapa inicial e crucial para gerenciar essa vulnerabilidade crítica e mitigar os riscos associados envolve a identificação de todos os ativos suscetíveis a esse problema específico.

Classificação: Público

Usando o CSAM com o Gerenciamento de Superfície de Ataque Externo para identificar as instâncias voltadas para a Internet da sua organização que têm versões vulneráveis do OpenSSH ou estão em seu Fim de Vida Útil (EOL) ou Fim de Suporte (EOS).

No exemplo a seguir, é possível identificar todos os ativos que executam o OpenSSH:

```
software:(name:"openssh" and version<4.4 and lifecycle.stage: `EOL/EOS`) or software:(name:"openssh" and version<9.8 and version>=8.5 and lifecycle.stage: `EOL/EOS`)
```

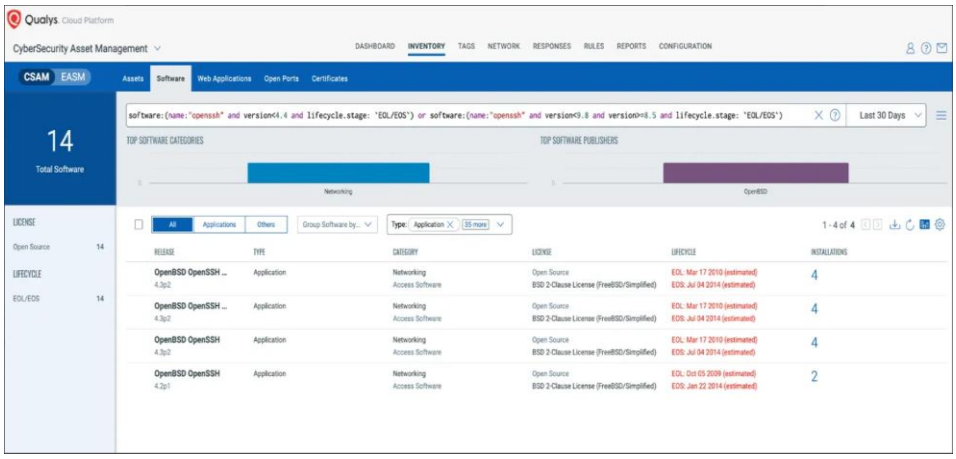

Figura 4 – CyberSecurity Asset Management do Qualys exibindo ativos com OpenSSH. Fonte: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

```
software:(name:"openssh" and version<4.4) or software:(name:"openssh" and version<9.8 and version>=8.5)
```

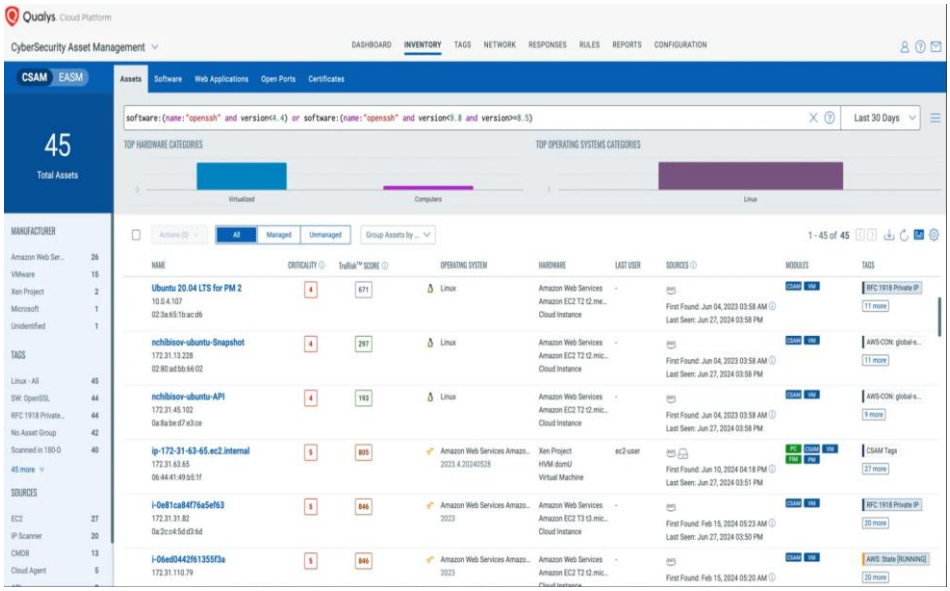

Figura 5 – CyberSecurity Asset Management do Qualys exibindo ativos com OpenSSH. Fonte: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

Melhora de postura de segurança com o Qualys Vulnerability Management, Detection, and Response (VMDR):

O Qualys VMDR oferece cobertura abrangente e visibilidade sobre vulnerabilidades, capacitando as organizações a responder, priorizar e mitigar rapidamente os riscos associados.

Classificação: Público

Além disso, os clientes da Qualys podem aproveitar o Qualys Patch Management para corrigir essas vulnerabilidades de forma eficaz.

Com o Qualys VMDR ao lado do TruRisk e da Qualys Query Language (QQL) para identificar e priorizar com eficiência ativos vulneráveis, abordando efetivamente as vulnerabilidades destacadas acima.

Use esta instrução QQL:

```
vulnerabilities.vulnerability.cveIds:CVE-2024-6387
```

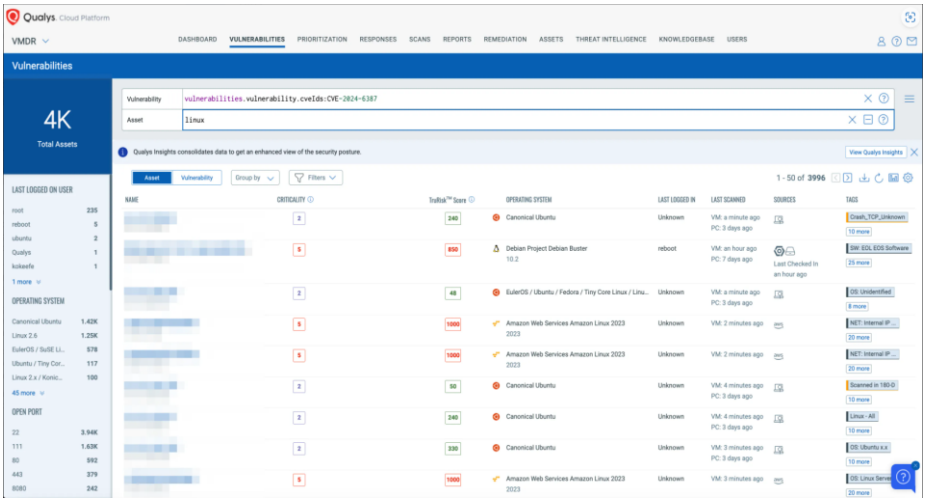

Figura 6 – VMDR do Qualys exibindo ativos com a CVE-2024-6387. Fonte: https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

Detectar e corrigir CVE-2024-6387 com o Qualys TotalCloud Container Security:

O Qualys TotalCloud Container Security oferece cobertura abrangente e visibilidade de vulnerabilidades em todos os seus ambientes de contêiner, incluindo Kubernetes gerenciados e Kubernetes locais. Isso permite que as organizações respondam, priorizem e mitiguem rapidamente os riscos associados de forma eficaz.

É possível utilizar o Qualys TotalCloud Container Security junto ao Qualys Query Language (QQL) para identificar e priorizar com eficiência ativos vulneráveis, garantindo a correção rápida e eficaz das vulnerabilidades destacadas pelo CVE-2024-6387.

Use esta instrução QQL:

```
state:`RUNNING` and vulnerabilities.cveids:CVE-2024-6387
```

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://nvd.nist.gov/vuln/detail/CVE-2024-6387 e https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

2.4. Recente vulnerabilidade no protocolo RADIUS, torna redes expostas a ataque man-in-the-middle

Pesquisadores de segurança cibernética descobriram uma vulnerabilidade no protocolo de autenticação de rede RADIUS, chamada BlastRADIUS. Essa falha pode ser explorada por invasores para realizar ataques Man-in-the-middle (MitM) e ignorar verificações de integridade em determinadas situações.

Classificação: Público

Esta vulnerabilidade foi atribuída com o CVE-2024-3596 e ainda se encontra sem classificação pelo NIST, ela possui a seguinte descrição “O protocolo RADIUS sob RFC 2865 é suscetível a ataques de falsificação por um invasor local que pode modificar qualquer resposta válida (acesso-aceito, acesso-rejeitado ou acesso-desafio) para qualquer outra resposta usando um ataque de colisão de prefixo escolhido contra a assinatura do autenticador de resposta MD5.”

A segurança do RADIUS depende de um hash derivado do algoritmo MD5, que foi considerado criptograficamente comprometido em dezembro de 2008 devido ao risco de ataques de colisão. Isso significa que os pacotes de solicitação de acesso podem ser alvo de um ataque de prefixo escolhido, permitindo a modificação do pacote de resposta de forma que ele passe por todas as verificações de integridade da resposta original. No entanto, para que o ataque seja bem-sucedido, o adversário precisa ser capaz de modificar pacotes RADIUS em trânsito entre o cliente e o servidor. Isso implica que organizações que enviam pacotes pela internet estão em risco.

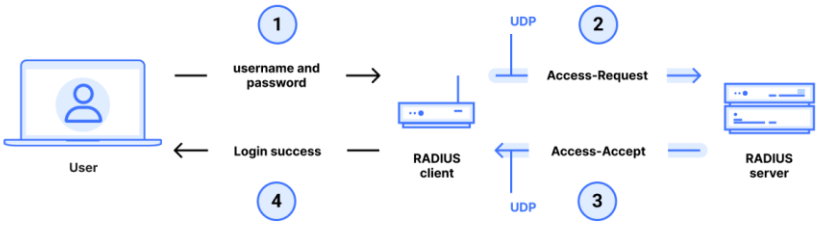

Figura 7 - RADIUS/UDP no modo Password Authentication Protocol (PAP). Esse ataque também se aplica aos modos de autenticação RADIUS/UDP CHAP e RADIUS/UDP MS-CHAP. Fonte: https://blog.cloudflare.com/radius-udp-vulnerable-md5-attack

Exploração

O invasor desta vulnerabilidade utiliza um ataque Man-in-the-Middle (MitM) entre um cliente RADIUS (por exemplo, um roteador) e um servidor RADIUS para alterar um pacote Access-Reject em um pacote Access-Accept, explorando vulnerabilidades no algoritmo MD5. Dessa forma, ele obtém acesso não autorizado ao roteador. O fluxo detalhado do ataque está ilustrado no diagrama abaixo.

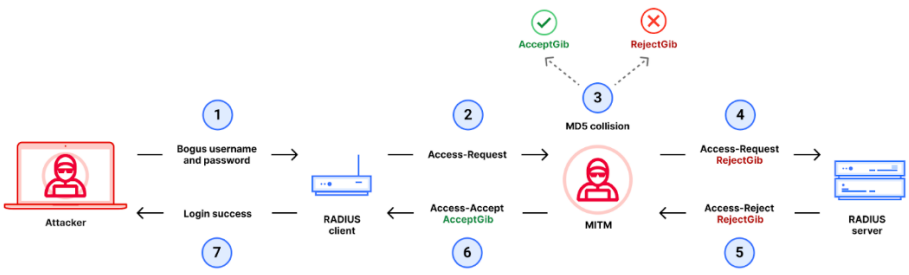

Figura 8 - Visão geral do ataque Blast-RADIUS em RADIUS/UDP no modo PAP. Fonte: https://blog.cloudflare.com/radius-udp-vulnerable-md5-attack

Primeiro, o invasor tenta fazer login no dispositivo em execução no cliente RADIUS usando um nome de usuário e senha falsos, o cliente RADIUS envia um pacote de solicitação de acesso que é interceptado pelo MitM.

Classificação: Público

Em seguida, o MitM executa um ataque de colisão de prefixo escolhido MD5 da seguinte maneira: O prefixo P1 corresponde a atributos hashed com MD5 para produzir o autenticador de resposta de um pacote Access-Reject. O prefixo P2 corresponde aos atributos de um pacote Access-Accept. O MitM pode prever P1 e P2 simplesmente olhando para o pacote Access-Request que interceptou. Em seguida, o atacante executa o ataque de colisão de prefixo escolhido MD5 para encontrar os dois blocos de bobagem, G1 (o RejectGib mostrado na figura acima) e G2 (o AcceptGib) para obter uma colisão MD5 entre P1 || RejectGib e P2 || AcceptGib.

O invasor coloca a colisão nos pacotes RADIUS, e para fazer isso, ele usa um atributo RADIUS/UDP opcional chamado Proxy-State. O Proxy-State é um lugar ideal para encher essa bagunça porque um servidor RADIUS deve ecoar todas as informações que recebe em um atributo Proxy-State do cliente RADIUS. O Proxy-State também deve ser hashed por MD5 no Response Authenticator da resposta correspondente. O MitM pega o RejectGib e o adiciona ao pacote Access-Request que o MitM interceptou como vários atributos Proxy-State. Para que isso funcione, ele garante que o gibberish de colisão (RejectGib e AcceptGib) seja formatado corretamente como vários atributos Proxy-State. Este é um novo aspecto criptográfico do ataque. Em seguida, ele explora o fato de que o servidor RADIUS irá ecoar de volta o gibberish em sua resposta.

O servidor RADIUS recebe a solicitação de acesso modificada e responde com um pacote de rejeição de acesso. Este pacote Access-Reject inclui os atributos Proxy-State que contêm o RejectGib e (b) um Autenticador de Resposta computado como MD5 (P1 || RejectGib || Secret). Observe que ele altera a entrada para o Autenticador de Resposta para ser uma das colisões MD5 encontradas pelo MitM.

Finalmente, o MitM intercepta o pacote Access-Reject, extrai o Response-Authenticator do pacote interceptado e o usa para forjar um pacote Access-Accept usando nossa colisão MD5. O pacote forjado é (a) formatado como um pacote Access-Accept que (b) tem o AcceptGib em Proxy-State e copia o Response Authenticator do pacote Access-Reject que o MitM interceptou do servidor.

O invasor usa o MD5 para substituir um Access-Reject por um Access-Accept, o pacote Access-Accept forjado chega ao cliente RADIUS, que o aceita porque entrada para o Autenticador de Resposta é P2 || AcceptGib, o Response-Authenticator é MD5 (P1 || RejectGib || Secret), o P1 || RejectGib é uma colisão MD5 com o P2 || AcceptGib, o que implica o MD5 (P1 || RejectGib || Secret) = MD5 (P2 || AcceptGib || Secret). Em outras palavras, o Response-Authenticator no pacote Access-Accept forjado é válido.

Mitigação e Prevenção

O RADIUS têm um atributo Message-Authenticator que usa HMAC-MD5 e é opcional para modos RADIUS/UDP que não usam EAP. A nova atenuação envolve tornar o Message-Authenticator um requisito para pacotes de solicitação e resposta para todos os modos de RADIUS/UDP. A mitigação funciona porque o Message-Authenticator usa HMAC-MD5, que não é suscetível ao ataque de colisão de prefixo escolhido MD5.

O destinatário de qualquer pacote RADIUS/UDP deve sempre exigir que o pacote contenha um Message-Authenticator e deve validar o HMAC-MD5 no Message-Authenticator. Os servidores RADIUS devem enviar o Message-Authenticator como o primeiro atributo em cada resposta Access-Accept ou Access-Reject enviada pelo servidor RADIUS.

Há algumas coisas a serem observadas ao aplicar esse patch na prática. Como o RADIUS é um protocolo cliente-servidor, é preciso considerar a eficácia do patch se ele não for aplicado uniformemente a todos os clientes e servidores RADIUS e o risco de o patch quebrar a compatibilidade cliente-servidor.

Classificação: Público

Corrigir apenas o cliente não impede ataques, porque a atenuação exige que o remetente inclua um Message-Authenticator no pacote, e o destinatário exija que um Message-Authenticator esteja presente no pacote e o valide. Em outras palavras, tanto o cliente quanto o servidor precisam mudar seus comportamentos. Se o destinatário não exigir que o Message-Authenticator esteja presente no pacote, o MitM poderá fazer um ataque de downgrade em que retira o Message-Authenticator do pacote e o ataque ainda funcionaria. Enquanto isso, há algumas evidências de que a aplicação de patches apenas no servidor pode ser mais eficaz, devido à mitigação, enviando o Message-Authenticator como o primeiro atributo no pacote de resposta.

É improvável que a implantação do patch em clientes quebre a compatibilidade, porque as especificações RADIUS há muito exigem que os servidores RADIUS devem ser capazes de processar qualquer atributo Message-Authenticator enviado por um cliente RADIUS. Dito isso, não podemos descartar a existência de servidores RADIUS que não estejam em conformidade com esse aspecto de longa data da especificação, por isso é sugerido testar os servidores RADIUS antes de aplicar patches nos clientes.

Por outro lado, aplicar patches no servidor sem quebrar a compatibilidade com clientes herdados pode ser mais complicado. Os servidores RADIUS comerciais são construídos principalmente em uma de um pequeno número de implementações (como FreeRADIUS), e as implementações mantidas ativamente devem estar atualizadas sobre mitigações. No entanto, há um conjunto mais amplo de implementações de cliente RADIUS, algumas das quais são herdadas e difíceis de corrigir.

Se um cliente herdado sem patch não souber como enviar um atributo do Autenticador de Mensagem, o servidor não poderá exigi-lo desse cliente sem interromper a compatibilidade com versões anteriores. A conclusão é que, para que tudo isso funcione, é importante corrigir servidores e clientes.

Isolar o tráfego RADIUS é há muito tempo uma prática recomendada para evitar o envio de tráfego RADIUS/UDP ou RADIUS/TCP de forma clara pela Internet pública. Em redes internas, recomenda-se isolar o tráfego RADIUS em uma VLAN de gerenciamento de acesso restrito ou túnelá-lo por TLS ou IPsec. Isso é útil porque dificulta o acesso dos invasores ao tráfego RADIUS, tornando mais difícil a execução de ataques. No entanto, um invasor ainda pode realizar um ataque de escalonamento de privilégios se uma configuração incorreta ou comprometimento da rede permitir que um MitM (Man-in-the-Middle) acesse o tráfego RADIUS.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://blog.cloudflare.com/radius-udp-vulnerable-md5-attack , https://thehackernews.com/2024/07/radius-protocol-vulnerability-exposes.html e https://nvd.nist.gov/vuln/detail/CVE-2024-3596

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

A publicação do documento de Inteligência de Ameaças será realizada quinzenalmente.

Produzido por: Comitê Editorial de Segurança da Service Sec

Contato, sugestões e críticas: comite.editorial@servicesec.com.br

Classificação: Público