Your IT Company

Principais Vulnerabilidades e Ameaças (Agosto/24)

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Uma falha no Windows Smart App Control e no SmartScreen permite que hackers sequestrem sistemas. 2
2.2. Vulnerabilidades recentes no ServiceNow permitem a execução remota de códigos arbitrários. 6
2.3. Uma falha nos roteadores VPN da Cisco permite que invasores executem código arbitrário remotamente 12
2.4. Uma vulnerabilidade em papéis de parede permite que atacantes realizem elevação de privilégio em sistemas Windows. 14

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.

2. Vulnerabilidades e Ameaças descobertas

2.1. Uma falha no Windows Smart App Control e no SmartScreen permite que hackers sequestrem sistemas.

O Microsoft SmartScreen tem sido um recurso incorporado no sistema operacional desde o Windows 8. Ele opera em arquivos que possuem a "Marca da Web" (MotW) e são clicados pelos usuários. A Microsoft introduziu o Smart App Control (SAC) com o lançamento do Windows 11. O SAC é, em alguns aspectos, uma evolução do SmartScreen. A Microsoft afirma que ele “adiciona proteção significativa contra novas e emergentes ameaças, bloqueando aplicativos que são maliciosos ou não confiáveis.” Ele funciona consultando um serviço em nuvem da Microsoft quando os aplicativos são executados. Se forem conhecidos por serem seguros, são permitidos para execução; no entanto, se forem desconhecidos, serão executados apenas se tiverem uma assinatura de código válida. Quando o SAC está ativado, ele substitui e desativa o Defender SmartScreen.

Hackers recentemente vem explorando falhas de segurança no Windows Smart App Control e SmartScreen para lançar códigos e aplicativos maliciosos.

Os atores de ameaças que visam minar os recursos de segurança do Windows podem usar essas vulnerabilidades para obter acesso, roubar dados sensíveis e comprometer a integridade do sistema. Pesquisadores de cibersegurança descobriram que as vulnerabilidades no Windows Smart App Control e no SmartScreen permitem também que hackers sequestrem sistemas.

Exploração

Uma maneira de contornar o Smart App Control é simplesmente assinar o malware com um certificado de assinatura de código. Mesmo antes do SAC, havia uma tendência de os atacantes assinarem seus malwares para evitar a detecção. Mais recentemente, os atacantes têm rotineiramente obtido certificados de assinatura de Validação Estendida (EV). Os certificados EV exigem prova de identidade para obter acesso e só podem existir em tokens de hardware especialmente projetados, o que os torna difíceis de roubar. No entanto, os atacantes encontraram maneiras de se passar por empresas e comprar esses certificados. O grupo de ameaças por trás do SolarMarker utilizou mais de 100 certificados de assinatura únicos em suas campanhas. As Autoridades Certificadoras (CAs) deveriam fazer mais para reprimir o abuso e minimizar a aquisição fraudulenta de certificados. Mais pesquisas públicas podem ser necessárias para pressionar as CAs que mais frequentemente vendem certificados fraudulentos.

O sequestro de reputação é um paradigma de ataque genérico contra sistemas de proteção contra malwares baseados em reputação. É análogo à pesquisa de confiança mal colocada contra sistemas de controle de aplicativos, bem como à pesquisa de drivers vulneráveis. Infelizmente, a superfície de ataque, neste caso, é ainda maior. O sequestro de reputação envolve encontrar e reutilizar aplicativos com boa reputação para contornar o sistema. Para funcionar como um vetor de acesso inicial, uma restrição é que o aplicativo deve ser controlado sem quaisquer parâmetros de

Classificação: Público

linha de comando, um host de script que carrega e executa um script em um caminho de arquivo previsível.

Hosts de script são um alvo ideal para um ataque de sequestro de reputação. Isso é especialmente verdadeiro se incluírem uma interface de função estrangeira (FFI). Com FFI, os atacantes podem facilmente carregar e executar código arbitrário e malware na memória. Por meio de pesquisas no VirusTotal e no GitHub, foi identificado muitos hosts de script que têm uma boa reputação e podem ser cooptados para execução completa de código. Isso inclui interpretadores Lua, Node.js e AutoHotkey. Um exemplo para demonstrar essa técnica está disponível aqui (https://github.com/joe-desimone/rep-research/blob/ea8c70d488a03b5f931efa37302128d9e7a33ac0/rep-hijacking/poc-rep-hijack-jam.zip).

O gif a seguir demonstra o sequestro com a utilidade de construção JamPlus (https://github.com/jamplus/jamplus) para contornar o Smart App Control sem alertas de segurança:

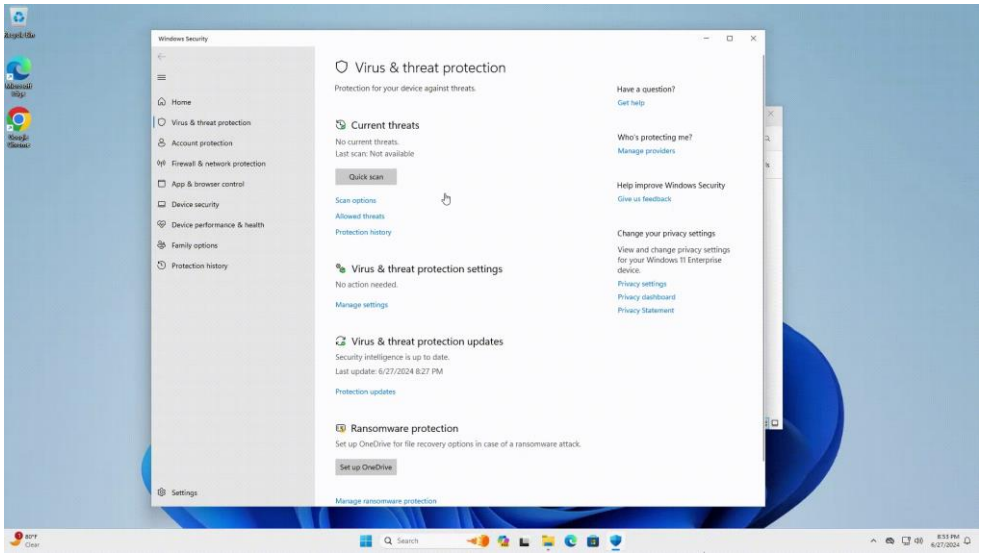

Figura 1 – Gif demonstrando o exploit. Fonte: https://www.elastic.co/security-labs/dismantling-smart-app-control

Em outro exemplo, os alertas de segurança do SmartScreen foram contornados usando um interpretador AutoHotkey conhecido:

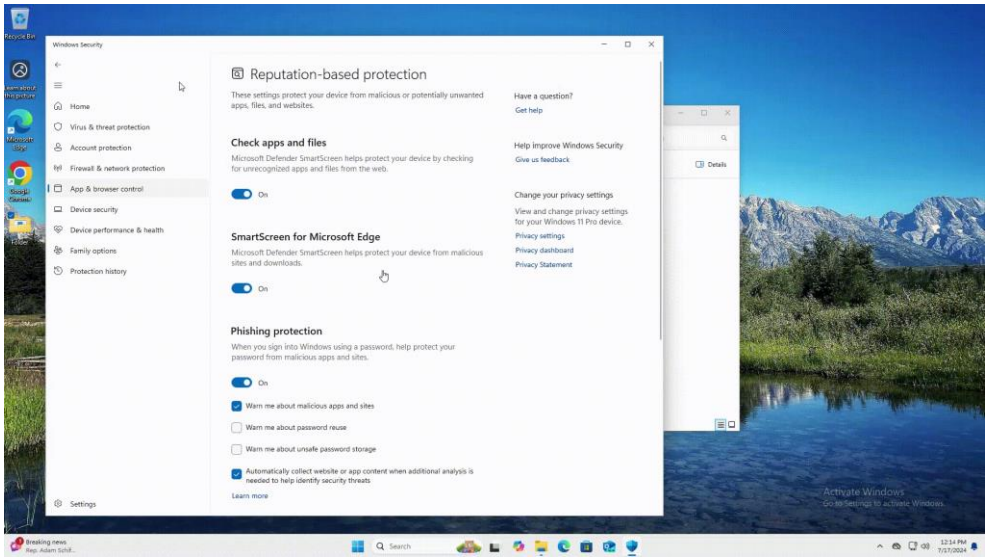

Figura 2 – Gif demonstrando um segundo exploit. Fonte: https://www.elastic.co/security-labs/dismantling-smart-app-control

Classificação: Público

Outra forma de sequestrar a reputação de um aplicativo conhecido é explorá-lo. Isso pode ser simples, como um estouro de buffer clássico ao ler um arquivo INI em um caminho previsível. Pode ser algo mais complexo que se encadeia com outras primitivas (como execução de comandos/escrita no registro/etc.). Além disso, vários aplicativos conhecidos podem ser encadeados juntos para alcançar a execução completa de código. Por exemplo, um aplicativo que lê um arquivo de configuração e executa um parâmetro de linha de comando pode ser usado para lançar outro aplicativo conhecido que requer um conjunto de parâmetros para obter execução arbitrária de código.

Outro ataque contra proteções baseadas em reputação é semear binários controlados por atacantes no sistema. Se forem cuidadosamente elaborados, esses binários podem parecer benignos e obter uma boa reputação, ao mesmo tempo que são úteis para os atacantes posteriormente. Pode ser simplesmente um novo binário de host de script, um aplicativo com uma vulnerabilidade conhecida ou um aplicativo que tem uma primitiva útil. Por outro lado, pode ser um binário que contém código malicioso embutido, mas que só é ativado após uma determinada data ou gatilho ambiental.

O Smart App Control parece vulnerável ao seeding. Após executar uma amostra em uma máquina, ela recebeu um rótulo positivo após aproximadamente 2 horas. Foi observado que técnicas básicas de anti-emulação pareciam ser um fator para receber um veredicto ou reputação benignos. Felizmente, o SmartScreen parece ter um nível de prevalência global mais alto antes de confiar em um aplicativo. Uma amostra que demonstra essa técnica está disponível no link a seguir (https://github.com/joe-desimone/rep-research/blob/ea8c70d488a03b5f931efa37302128d9e7a33ac0/rep-seeding/poc-rep-seeding.zip) e é demonstrada abaixo:

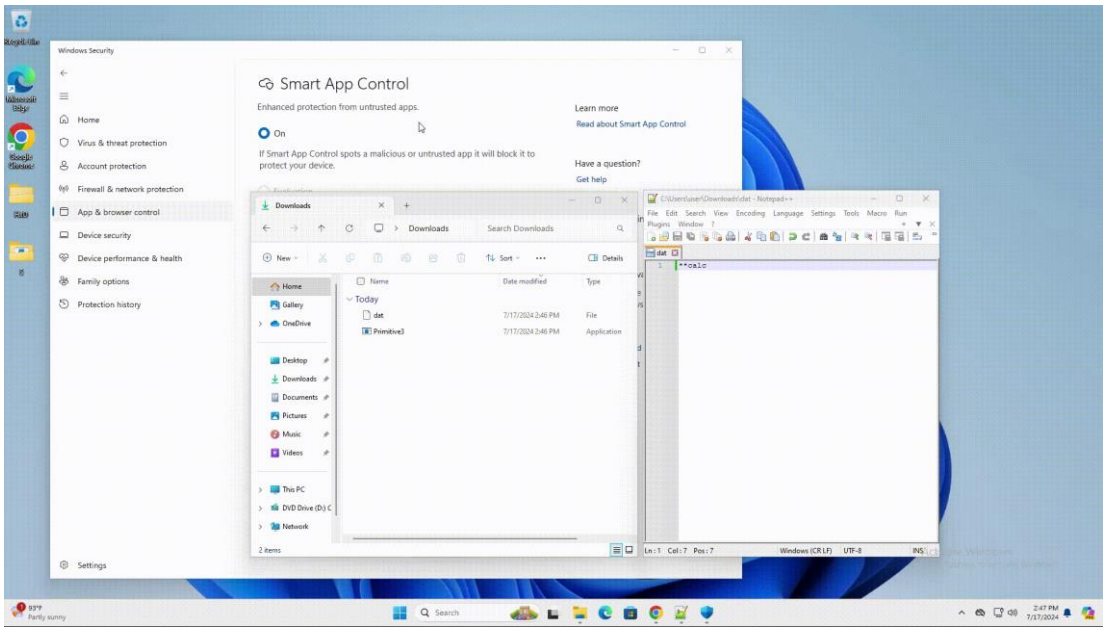

Figura 3 – Gif demonstrando exploit seeding de reputação. Fonte: https://www.elastic.co/security-labs/dismantling-smart-app-control

Uma terceira classe de ataque contra sistemas de reputação é a manipulação de reputação. Normalmente, sistemas de reputação usam sistemas de hash criptograficamente seguros para tornar a manipulação inviável. No entanto, os pesquisadores notaram que certas modificações em um arquivo não pareciam alterar a reputação para o SAC. O SAC pode usar hashing difuso ou comparações de similaridade baseadas em características em vez de, ou além de, hashing de arquivos padrão. Também pode alavancar um modelo de ML na nuvem para permitir arquivos que

Classificação: Público

tenham uma pontuação altamente benigna (como ser muito semelhante a algo conhecido como bom). Surpreendentemente, algumas seções de código poderiam ser modificadas sem perder sua reputação associada. Por meio de tentativa e erro, conseguiram identificar segmentos que poderiam ser adulterados com segurança e manter a reputação. Foi criado um binário adulterado (https://github.com/joe-desimone/rep-research/blob/ea8c70d488a03b5f931efa37302128d9e7a33ac0/rep-tampering/poc-rep-tampering.zip) com um hash único que nunca tinha sido visto pela Microsoft ou pelo SAC. Este embutiu um shellcode de "executar calc" e poderia ser executado com o SAC em modo de aplicação:

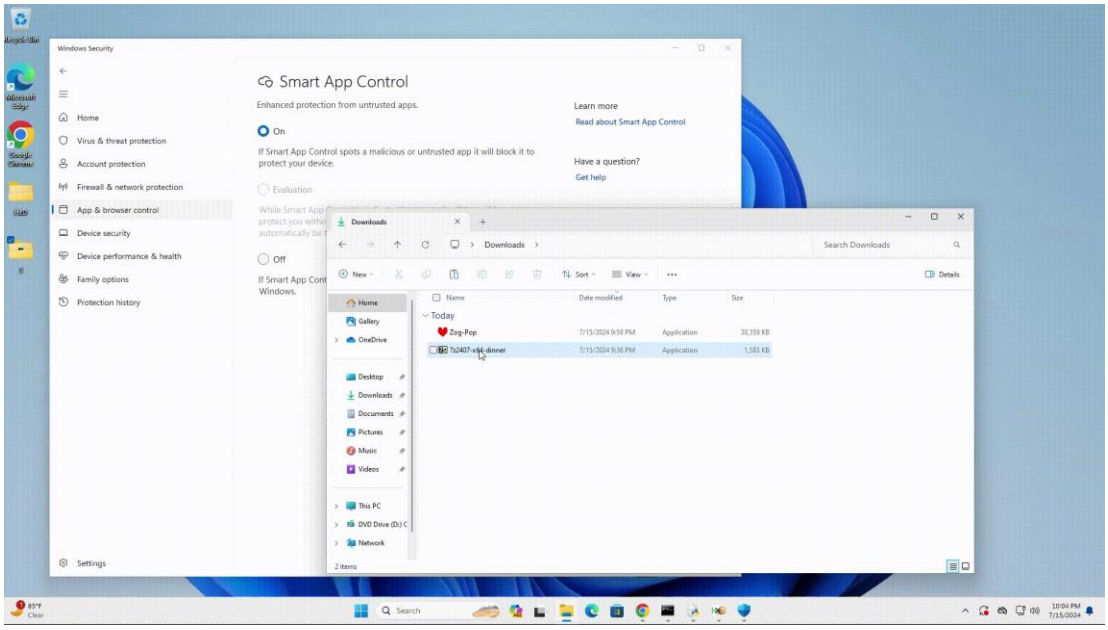

Figura 4 – Gif demonstrando exploit manipulação de reputação. Fonte: https://www.elastic.co/security-labs/dismantling-smart-app-control

Mitigação e prevenção usando Qualys e Trend Micro

Qualys

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras detalhadas em sistemas que utilizam o Smart App Control.
- Identifique quaisquer modificações ou desabilitações não autorizadas do Smart App Control usando Qualys File Integrity Monitoring (FIM).
- Identifique rapidamente os sistemas vulneráveis e priorize a correção utilizando o recurso de priorização de ameaças do Qualys.
- Reforce as configurações do Smart App Control de acordo com as melhores práticas de segurança.
- Automatize a aplicação de políticas de conformidade e correção com o Qualys Policy Compliance.
- Habilite o monitoramento contínuo com o Qualys para detectar mudanças não autorizadas nas configurações de segurança.
- Configure alertas para quaisquer tentativas de desabilitação ou modificação do Smart App Control.

Classificação: Público

Trend Micro

- Utilize o Trend Micro Vision One para monitorar e impedir modificações não autorizadas nas configurações de segurança, incluindo o Smart App Control.
- Aplique regras de prevenção de intrusão (IPS) para detectar e bloquear tentativas de exploração dessa vulnerabilidade.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas, como tentativas de desabilitar ou modificar o Smart App Control.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas relacionadas a essa vulnerabilidade.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para ações rápidas e coordenadas.
- Utilize playbooks de resposta automática para restaurar configurações de segurança comprometidas e conter ameaças.
- Eduque os usuários sobre a importância de manter o Smart App Control ativado e sobre os riscos associados à desativação desse recurso.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.elastic.co/security-labs/dismantling-smart-app-control e https://cybersecuritynews.com/windows-smart-app-control-smartscreen-flaw/

2.2. Vulnerabilidades recentes no ServiceNow permitem a execução remota de códigos arbitrários.

A ServiceNow, é uma plataforma de automação de fluxos de trabalho que oferece uma ampla gama de soluções para gerenciar e otimizar processos empresariais. Ele é mais conhecido por seu módulo de IT Service Management (ITSM), que ajuda organizações a gerenciar incidentes, problemas, mudanças e solicitações de serviços de TI de forma eficiente, a empresa divulgou recentemente duas vulnerabilidades críticas de segurança que podem ter consequências graves para as organizações que a utilizam em todo o mundo. Essas vulnerabilidades afetam várias versões do Now Plataform, incluindo as versões de Washington DC, Vancouver e Utah.

As vulnerabilidades estão identificadas como CVE-2024-4879 e CVE-2024-5217 ambas classificadas pela ServiceNow utilizando a CVSS 4.0: 9.3 e 9.2 de nível crítico e com a descrição: “A ServiceNow corrigiu uma vulnerabilidade de validação de entrada que foi identificada nas versões Vancouver e Washington DC da plataforma Now. Essa vulnerabilidade poderia permitir que um usuário não autenticado executasse remotamente código no contexto da plataforma Now. A ServiceNow aplicou uma atualização para as instâncias hospedadas e lançou a atualização para seus parceiros e clientes com instâncias autogerenciadas.” As duas vulnerabilidades não tiveram classificação realizada pela NIST.

Essas vulnerabilidades permitem que invasores remotos não autenticados executem código arbitrário na Now Platform, potencialmente levando ao comprometimento, roubo de dados e interrupção das operações de negócios.

Estimar com precisão é difícil, mas o ServiceNow é uma plataforma amplamente utilizada para gerenciar fluxos de trabalho digitais em ambientes de TI modernos. Por exemplo, com base nos resultados de um mecanismo de pesquisa de rede popular na China, chamado FOFA que é uma

Classificação: Público

ferramenta de inteligência cibernética e motor de busca que permite aos usuários realizar buscas em larga escala por dispositivos e serviços expostos na internet, existem aproximadamente 300.000 instâncias do ServiceNow que podem ser investigadas remotamente.

Naturalmente, essas instâncias podem ter diferentes ACLs (listas de controle de acesso) ou outras limitações de acesso no nível da rede e do aplicativo, o que significa que só podem ser usadas para uma estimativa aproximada. Ainda assim, isso confirma a ampla e significativa penetração dessa solução em ambientes corporativos ao redor do mundo. O maior número de casos foi identificado nos Estados Unidos, Reino Unido, Índia e União Europeia.

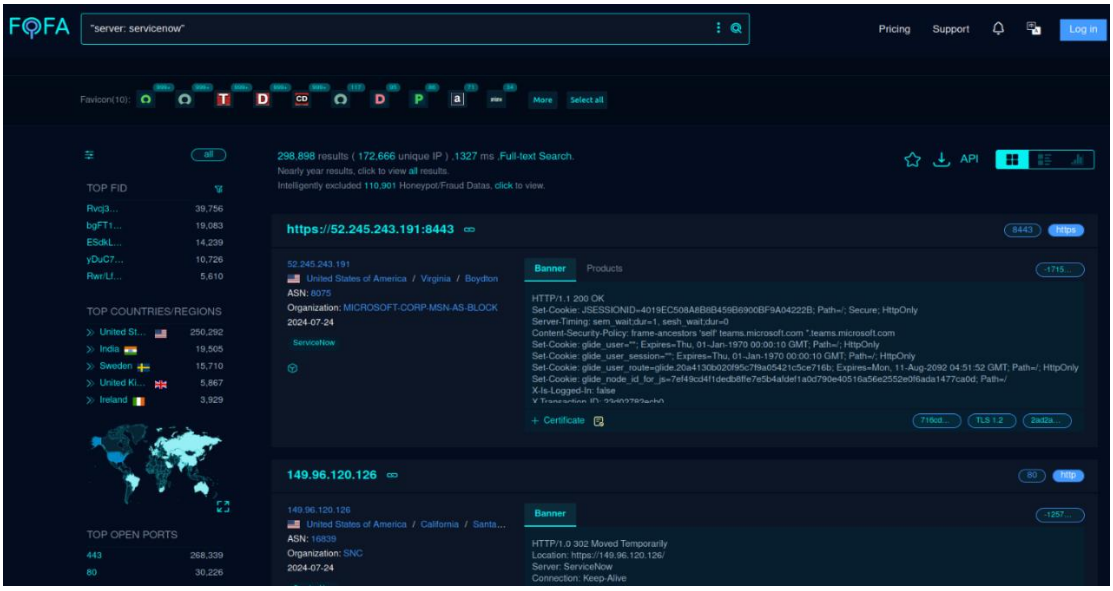

Figura 5 - Mecanismos de pesquisa de rede popular FOFA. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Outros mecanismos de pesquisa frequentemente usados por adversários para mapeamento de rede e identificação rápida de hosts também mostraram um número significativo de acessos, variando entre 13.300 e 23.000 hosts de rede.

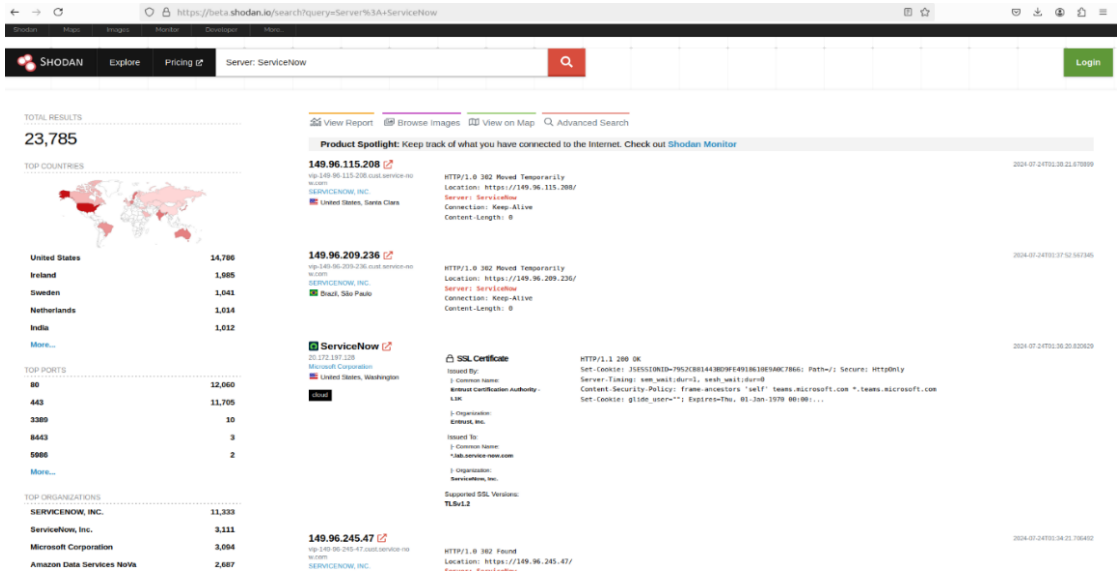

Figura 6 - Mecanismo de pesquisa Shodan. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Classificação: Público

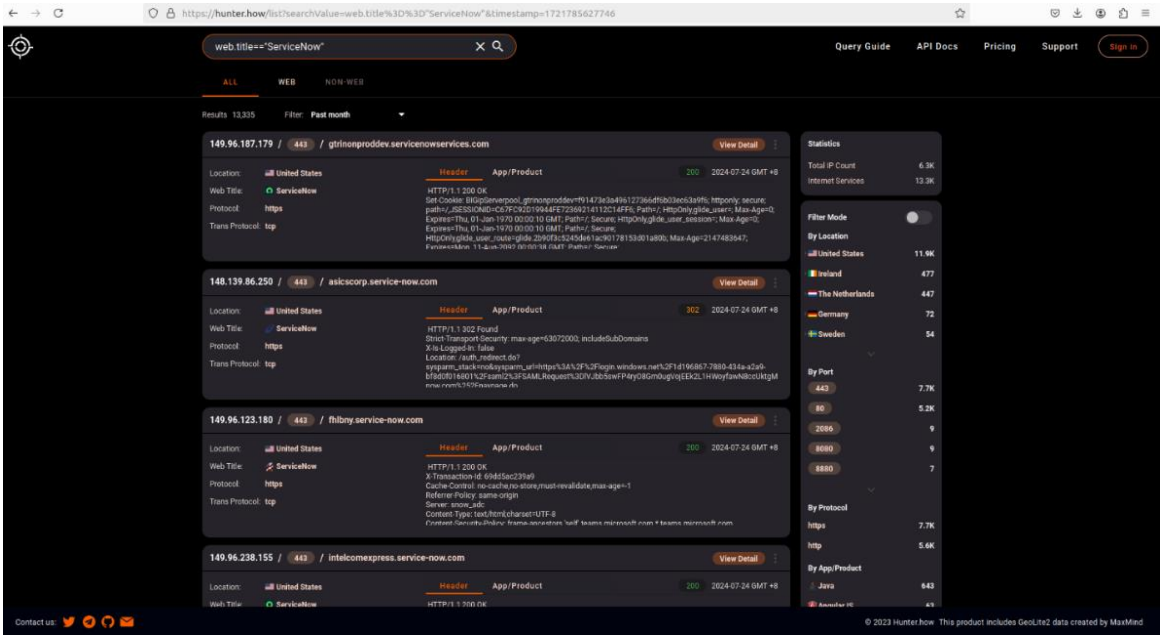

Figura 7 – Mecanismo de pesquisa Hunternow. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

O número real de hosts mapeados pode variar, mas mesmo assim, os adversários têm uma janela de oportunidade para explorar vulnerabilidades em aplicativos populares antes que os patches sejam aplicados. Dependendo da configuração, essa atividade pode ter um impacto limitado ou significativo, e os mecanismos de pesquisa que permitem a descoberta de aplicativos corporativos são amplamente utilizados indevidamente pelos invasores. Duas dessas listas (usadas para realizar a verificação) foram adquiridas pelos pesquisadores.

Os mecanismos de varredura e detecção utilizados por esses mecanismos de pesquisa (mencionados acima) são proprietários e podem ser esclarecidos diretamente com seus autores. Na maioria dos casos, esses mecanismos utilizam bots e ferramentas de verificação específicas para examinar o espaço de endereços, com o objetivo de coletar assinaturas de servidores web, aplicativos, serviços de rede e dispositivos de rede/IoTs. Essas informações, quando disponibilizadas publicamente, também são mal utilizadas pelos adversários, permitindo que eles naveguem rapidamente para possíveis correspondências relevantes às suas áreas de interesse.

Exploração

Assim que as informações sobre vulnerabilidades foram divulgadas, diversos agentes de ameaças imediatamente iniciaram varreduras em massa para identificar instâncias vulneráveis do ServiceNow. Pesquisadores monitoraram de perto vários desses atores, permitindo coletar contexto suficiente sobre seu modus operandi (MO). O catalisador para a exploração foi a divulgação pública de uma prova de conceito (PoC) com o objetivo de conscientizar sobre segurança cibernética. Um dos CVEs mais investigados ativamente por agentes de ameaças foi o CVE-2024-4879, que permite a execução remota de código por um usuário não autenticado na Now Platform. Essa vulnerabilidade explora três problemas encadeados: injeção de título, desvio de mitigação de injeção de modelo e desvio de filtro do sistema de arquivos para acessar dados do ServiceNow. Na prática, essas solicitações também podem ser usadas separadamente.

Durantes analises os sensores de rede utilizados pelos pesquisadores registraram várias solicitações de sondagem, permitindo que os invasores confirmem se uma instância específica do ServiceNow estava vulnerável antes de explorá-la ativamente. Inicialmente, os agentes de ameaças

Classificação: Público

estavam injetando uma carga útil e verificando se havia um resultado de multiplicação específico na resposta:

```
/login.do?jvar_page_title=%3Cstyle%3E%3Cj:jelly%20xmlns:j=%22jelly%22%20xmlns:g=%27glide%27%3E%3Cg:evaluate%3Egs.addErro
```

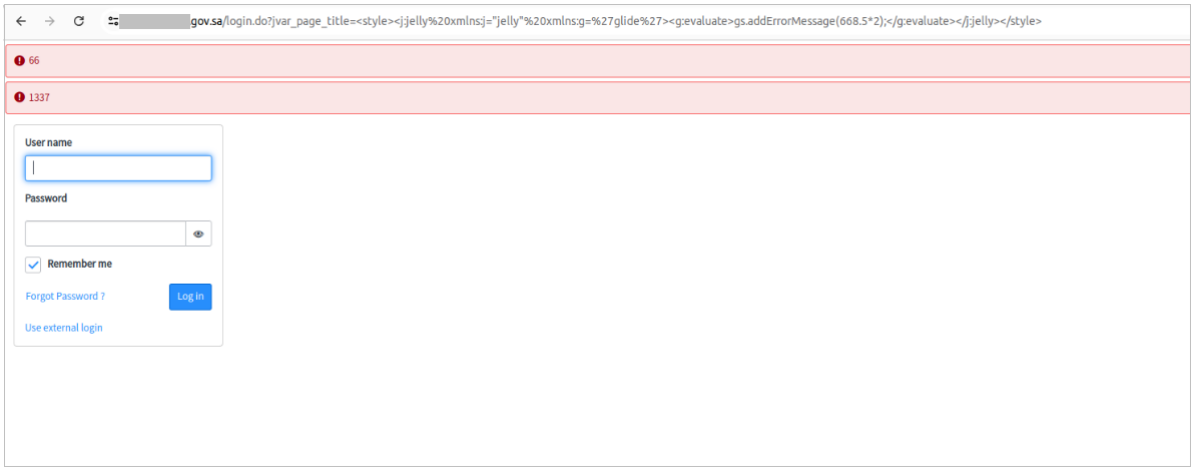

Figura 8 - Registro de sensores. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

O segundo estágio de exploração envolveu a injeção de uma carga útil para verificar a disponibilidade e o conteúdo do banco de dados. Isso pode ser orquestrado manualmente enviando a seguinte solicitação ou usando modelos personalizados para scanners populares para automação, como Nuclei, com modelo adicionado recentemente para CVE-2024-5217 em seu repositório:

```
/login.do?jvar_page_title=%3Cstyle%3E%3Cj:jelly%20xmlns:j=%22jelly:core%22%20xmlns:g=%27glide%27%3E%3Cg:evaluate
%3Ez=new%20Packages.java.io.File(%22%22).getAbsolutePath(); z=z.substring(0,z.lastIndexOf(%22/%22));
u=new%20SecurelyAccess(z.concat(%22/co.. nf
glide.db.properties%22)).getBufferedReader(); s=%22%22; while((q=u.readLine())!==null)s=s.concat(q,%22%5Cn%22);
gs.addErrorMessage(s);%3C/g:evaluate%3E%3C/j:jelly%3E%3C/style%3E%22
```

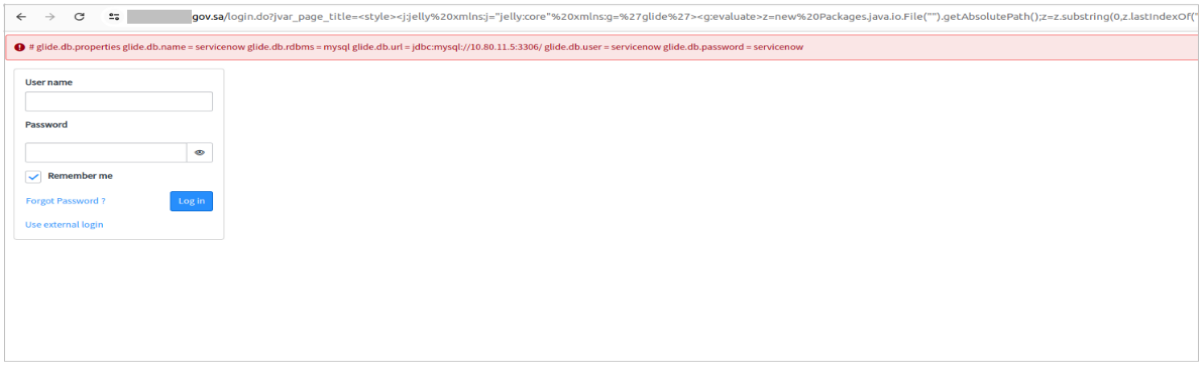

Figura 9 – Segunda fase do exploit. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Se a exploração for bem-sucedida, a instância vulnerável retornará detalhes sobre o banco de dados:

Classificação: Público

Figura 10 – Detalhes do banco de dados. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

O estágio final envolveu o despejo de listas de usuários e a coleta de metadados associados de instâncias comprometidas:

```
/login.do?jvar_page_title=<style><j:jelly xmlns:j="jelly" xmlns:g='glide'><g:evaluate>gr=new GlideRecord("sys_user");
gr.query(); s=""; while(gr.next())s=s.concat(gr.user_name," : ",gr.user_password,"<br/>"); gs.addErrorMessage(s);
</g:evaluate></j:jelly></style>
```

Figura 11 – Lista de usuários e dados coletados. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Na maioria dos casos, os dados coletados foram criptografados.

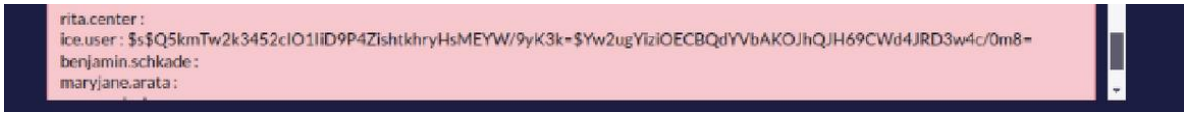

Figura 12 – Dados criptografados coletados. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Classificação: Público

Em análises realizadas os atacantes ainda não tiveram sucesso em quebrar a maioria dos hashes devido à complexidade do algoritmo utilizado, no entanto, as informações divulgadas podem facilitar os esforços de reconhecimento.

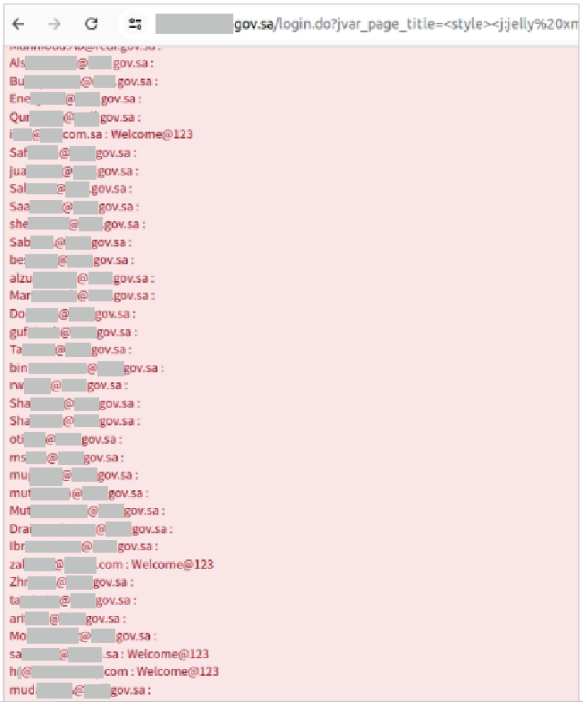

Figura 12 – Logins sem senhas, devido ao hash. Fonte: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign

Mitigação

A ServiceNow lançou patches e hotfixes para resolver essas vulnerabilidades. É crucial que as organizações que usam o ServiceNow apliquem essas atualizações imediatamente para proteger seus sistemas e dados contra possíveis ataques:

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648312

Mitigação e prevenção utilizando Qualys e Trend Micro

Qualys

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras completas em todos os ambientes ServiceNow.
- Identifique as instâncias vulneráveis utilizando a biblioteca de assinaturas de vulnerabilidades do Qualys que cobre CVE-2024-4879 e CVE-2024-5217.
- Utilize o recurso de priorização de ameaças do Qualys para identificar e focar nas instâncias mais críticas e vulneráveis.
- Aplique os patches e atualizações de segurança recomendados pela ServiceNow imediatamente após a identificação.

Classificação: Público

- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todas as correções sejam aplicadas de forma rápida e consistente.
- Habilite a monitoração contínua com o Qualys para detectar novas vulnerabilidades em tempo real.
- Configure alertas para qualquer atividade suspeita ou mudanças de configuração nos sistemas ServiceNow.

Trend Micro

- Utilize o Trend Micro Vision One para proteger as instâncias do ServiceNow contra exploração dessas vulnerabilidades, aplicando proteção contra exploits conhecidos.
- Configure regras de prevenção de intrusão (IPS) para detectar e bloquear tentativas de exploração de CVE-2024-4879 e CVE-2024-5217.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas nos servidores ServiceNow, especialmente aquelas que possam indicar tentativas de exploração RCE.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas que possam estar relacionadas a essas vulnerabilidades.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para ações rápidas e coordenadas, assegurando a contenção de ameaças e mitigação de danos.
- Utilize playbooks de resposta automática para isolar sistemas comprometidos e restaurar rapidamente as operações normais.
- Reforce as configurações de segurança do ServiceNow, garantindo que as práticas recomendadas sejam seguidas, como o uso de autenticação multifator (MFA) e restrições de acesso baseadas em função (RBAC).
- Realize avaliações regulares de conformidade e segurança utilizando o Trend Micro Vision One para garantir que as configurações estejam em conformidade com as políticas de segurança corporativas.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign , https://nvd.nist.gov/vuln/detail/CVE-2024-4879 e https://nvd.nist.gov/vuln/detail/CVE-2024-5217

2.3. Uma falha nos roteadores VPN da Cisco permite que invasores executem código arbitrário remotamente.

A Cisco divulgou recentemente que seus roteadores VPN Gigabit Dual WAN RV340 e RV345 possuem uma falha significativa no módulo de upload. Essa vulnerabilidade pode permitir que um invasor remoto e autenticado execute código arbitrário em um dispositivo afetado.

Esta vulnerabilidade recebeu a identificação: CVE-2024-20416 sendo classificada de acordo com a Cisco com a pontuação CVSS v3.1: 6.5 de nível médio e está descrita como: “Uma vulnerabilidade no módulo de upload dos roteadores VPN Gigabit de WAN dupla Cisco RV340 e

RV345 pode permitir que um invasor remoto autenticado execute código arbitrário em um dispositivo afetado. Essa vulnerabilidade ocorre devido a verificações de limite insuficientes ao processar solicitações HTTP específicas. Um invasor pode explorar essa vulnerabilidade enviando solicitações HTTP criadas para um dispositivo afetado. Uma exploração bem-sucedida pode permitir que o invasor execute código arbitrário como usuário root no sistema operacional subjacente do dispositivo". Até este momento a vulnerabilidade ainda está aguardando análise da NIST.

Produtos Cisco vulneráveis:

- Roteadores VPN Gigabit WAN Dual RV340
- RV340W Roteadores VPN Gigabit Wireless-AC WAN Dupla
- Roteadores VPN Gigabit WAN duplos RV345
- RV345P Roteadores VPN Gigabit PoE Dual WAN

A Cisco confirma que os seguintes produtos da Cisco não são afetados por essa vulnerabilidade:

- Roteadores VPN RV160
- Roteadores VPN sem fio AC RV160W
- Roteadores VPN RV260
- Roteadores VPN RV260P com PoE
- Roteadores VPN sem fio AC RV260W

A Cisco afirmou que não tem conhecimento de qualquer exploração de vulnerabilidade maliciosa ou anúncios públicos.

Esta vulnerabilidade permite que um invasor remoto não autenticado realize um ataque de força bruta para identificar combinações válidas de nome de usuário e senha. Com essas credenciais, o invasor pode estabelecer uma sessão VPN de acesso remoto não autorizada. Além disso, um invasor remoto autenticado pode estabelecer uma sessão VPN SSL sem cliente com um usuário não autorizado.

A vulnerabilidade está relacionada à separação inadequada de autenticação, autorização e contabilidade (AAA) entre o recurso VPN de acesso remoto e os recursos de gerenciamento HTTPS e VPN site a site. O invasor pode explorar essa falha especificando um perfil de conexão/grupo de túneis padrão durante um ataque de força bruta ou ao estabelecer uma sessão VPN SSL sem cliente usando credenciais válidas.

Mitigação e prevenção

Para mitigar essa vulnerabilidade, é recomendado atualizar para a versão mais recente do firmware fornecido pela Cisco. Além disso, é importante alterar a senha das contas locais que se conectam à VPN e exigir autenticação baseada em certificados digitais, desativando a autenticação por usuário e senha.

A prevenção envolve reforçar a orientação aos usuários sobre boas práticas de uso de credenciais e alertar sobre campanhas de phishing. É também importante manter seus dispositivos e sistemas atualizados para garantir a segurança de suas informações.

Mitigação e prevenção usando Qualys e Trend

Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras em todos os roteadores VPN Cisco na rede.

Classificação: Público

- Identifique as instâncias vulneráveis utilizando a biblioteca de assinaturas de vulnerabilidades do Qualys.
- Utilize o recurso de priorização de ameaças para focar nas instâncias mais críticas.
- Aplique patches e atualizações de firmware fornecidos pela Cisco imediatamente após a identificação.
- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todas as correções sejam aplicadas rapidamente e de forma consistente.
- Habilite a monitoração contínua do Qualys para detectar novas vulnerabilidades em tempo real.
- Configure alertas para mudanças na configuração dos roteadores VPN Cisco.

Trend:

- Utilize o Trend Micro Deep Security para proteger os roteadores VPN Cisco, aplicando proteção contra exploits e vulnerabilidades conhecidas.
- Configure regras de prevenção de intrusão (IPS) específicas para detectar e bloquear tentativas de exploração desta vulnerabilidade.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas em roteadores Cisco.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para ações rápidas e coordenadas.
- Utilize playbooks de resposta automática para conter ameaças e mitigar danos.
- Garanta que os roteadores VPN Cisco estejam configurados com as melhores práticas de segurança, como o uso de senhas fortes e a desativação de serviços desnecessários.
- Realize avaliações regulares de configuração e conformidade utilizando o Trend Micro para assegurar que as configurações sejam mantidas de acordo com as políticas de segurança.
- Utilize a segmentação de rede para limitar o impacto potencial de uma exploração bem-sucedida.
- Aplique políticas de acesso restrito baseadas no princípio de menor privilégio.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/cisco-vpn-routers-flaw/ e https://nvd.nist.gov/vuln/detail/CVE-2024-20416

2.4. Uma vulnerabilidade em papéis de parede permite que atacantes realizem elevação de privilégio em sistemas Windows.

Uma falha crítica de segurança no mecanismo de manipulação de papel de parede do Windows foi descoberta. Ela permite que atacantes obtenham privilégios de nível de administrador em máquinas afetadas. Está vulnerabilidade recebeu a identificação: CVE-2024-38100 sendo classificada de acordo com a Microsoft com a pontuação CVSS v3.1: 7.8 de nível alto, apelidada de “FakePotato” e está descrita como: “Vulnerabilidade de Elevação de Privilégio no Windows File Explorer”, esta vulnerabilidade não recebeu classificação da NIST.

Classificação: Público

A vulnerabilidade “FakePotato” se aproveita uma falha em como o Windows processa arquivos de papel de parede. Manipulando certas propriedades de uma imagem de papel de parede especialmente criada, um atacante com acesso limitado a um sistema pode elevar seus privilégios aos da conta SYSTEM, efetivamente obtendo controle completo sobre a máquina.

Esta falha de segurança afetou várias versões do Windows Server, incluindo:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2022 23H2

Exploração

O exploit de prova de conceito (PoC), que foi desenvolvido por um analista de segurança, o publicou no GitHub, a publicação pode ser acessada neste link (https://github.com/Florian-Hoth/CVE-2024-38100-RCE-POC), demonstrou como atacantes poderiam explorar essa vulnerabilidade para obter acesso não autorizado às credenciais de usuários. O exploit funcionava da seguinte maneira:

1. O atacante cria um arquivo de imagem (por exemplo, PNG ou JPEG) que contém código malicioso. Este código é embutido de maneira a ser executado quando o Windows processa a imagem como papel de parede.
2. O arquivo é distribuído por meio de e-mails de phishing, downloads maliciosos, ou carregado em sites populares de compartilhamento de imagens. Quando o usuário define a imagem como papel de parede, o código é executado, explorando a vulnerabilidade para executar comandos arbitrários com altos privilégios.
3. Uma vez que a vulnerabilidade é explorada, o código malicioso pode utilizar métodos como o "FakePotato" para elevar os privilégios de um usuário regular para um administrador, permitindo o controle total do sistema. Isso inclui a capacidade de instalar malware, roubar informações sensíveis, ou alterar configurações críticas do sistema.

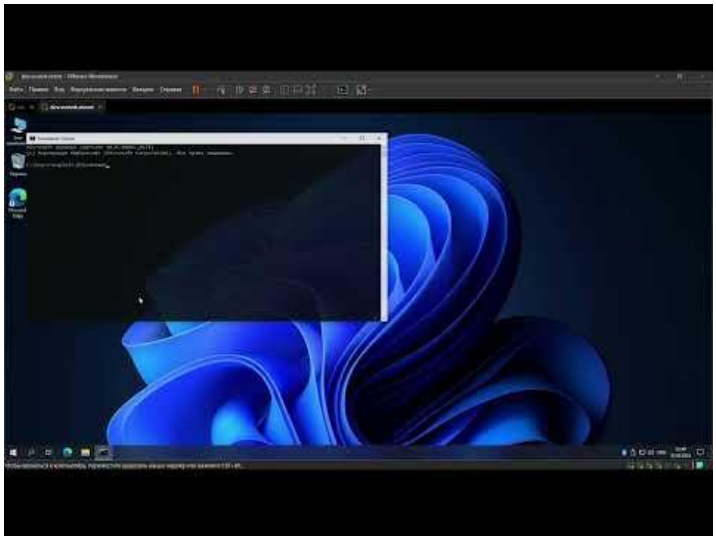

Figura 13 – Vídeo demonstrando como o exploit “FakePotato”’ funciona. Fonte: https://cybersecuritynews.com/leaked-wallpaper-exploit/

A exploração bem-sucedida dessa vulnerabilidade permite que atacantes:

- Elevação de privilégios em sistemas afetados.
- Obter acesso não autorizado a informações sensíveis de usuários.
- Movimentação lateral dentro de uma rede usando as credenciais obtidas.

Especialistas em segurança alertam que esse tipo de exploit pode ser particularmente perigoso em ambientes empresariais, onde o movimento lateral e a escalada de privilégios são componentes-chave de ameaças persistentes avançadas (APTs).

Mitigação e prevenção

A Microsoft já lançou uma atualização de segurança para abordar esta vulnerabilidade que recebeu a identificação: KB5040434, lançada em 9 de julho de 2024 (https://support.microsoft.com/pt-br/topic/9-de-julho-de-2024-kb5040434-compila%C3%A7%C3%A3o-do-sistema-operacional-14393-7159-40d1baef-65b4-467f-9bd9-729d369fcc4c).

É fortemente recomendado que usuários e administradores de sistemas apliquem esta atualização o mais rápido possível para mitigar o risco desta exploração.

Além disso, as organizações devem considerar implementar as seguintes medidas de segurança:

- Atualizar regularmente todos os sistemas e aplicativos Windows.
- Implementar o princípio de menor privilégio para contas de usuário.
- Monitorar atividades suspeitas relacionadas a tentativas de escalada de privilégios.
- Usar métodos de autenticação fortes e considerar a autenticação multifator sempre que possível.

Embora a Microsoft tenha corrigido essa vulnerabilidade específica, isso ressalta a importância de manter os sistemas atualizados e empregar práticas de segurança robustas para proteger contra ameaças emergentes.

Mitigação e prevenção usando Qualys e Trend

Qualys

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras detalhadas em todos os dispositivos que possam ser afetados por essa vulnerabilidade.
- Identifique sistemas que utilizam imagens potencialmente maliciosas como papéis de parede, utilizando a biblioteca de assinaturas de vulnerabilidades do Qualys.
- Utilize o recurso de priorização de ameaças do Qualys para focar nos sistemas mais críticos que estão utilizando papéis de parede ou imagens personalizadas.
- Implemente patches de segurança e atualizações fornecidas pelos fabricantes de sistemas operacionais para corrigir as falhas exploradas pelo "Leaked Wallpaper Exploit".
- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todas as correções sejam aplicadas de forma rápida e consistente.
- Habilite a monitoração contínua do Qualys para detectar novas vulnerabilidades e alterações suspeitas em tempo real.

Classificação: Público

- Configure alertas para identificar tentativas de exploração ou atividades anômalas relacionadas a imagens usadas como papéis de parede.

Trend Micro

- Utilize o Trend Micro Vision One para proteger os dispositivos contra o "Leaked Wallpaper Exploit", aplicando proteção contra exploits e vulnerabilidades conhecidas.
- Configure regras de prevenção de intrusão (IPS) para detectar e bloquear tentativas de exploração dessa vulnerabilidade através de imagens maliciosas.
- Use o recurso de análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas, como a alteração de papéis de parede ou o download de imagens de fontes não confiáveis.
- Monitore logs e eventos de segurança para identificar padrões de ataque e atividades anômalas que possam estar relacionadas ao uso de imagens como vetores de ataque.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para ações rápidas e coordenadas, assegurando a contenção de ameaças e mitigação de danos.
- Utilize playbooks de resposta automática para isolar dispositivos comprometidos e restaurar rapidamente as operações normais.
- Eduque os usuários sobre os riscos associados ao uso de papéis de parede de fontes não verificadas e a importância de utilizar apenas imagens confiáveis.
- Realize treinamentos regulares sobre a identificação de possíveis vetores de ataque, incluindo a utilização de imagens aparentemente inofensivas para explorar vulnerabilidades.
- Estabeleça políticas restritivas para o uso de papéis de parede personalizados em dispositivos corporativos, permitindo apenas o uso de imagens aprovadas e verificadas.
- Utilize ferramentas de controle de aplicações e políticas de restrição de conteúdo para prevenir o download e a aplicação de imagens potencialmente maliciosas.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/leaked-wallpaper-exploit/ , https://github.com/Florian-Hoth/CVE-2024-38100-RCE-POC e https://nvd.nist.gov/vuln/detail/CVE-2024-38100

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