Your IT Company

Principais Vulnerabilidades e Ameaças (Setembro/24)

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. Dez vulnerabilidades críticas identificadas na suíte de software QRadar da IBM.

O IBM QRadar Suite é uma poderosa plataforma de segurança cibernética que integra SIEM (Security Information and Event Management), SOAR (Security Orchestration Automation and Response), análise de tráfego de rede e gerenciamento de vulnerabilidades em uma solução unificada. Essa plataforma oferece detecção de ameaças, resposta a incidentes e gerenciamento de conformidade de forma integrada e eficiente.

A IBM emitiu um boletim de segurança destacando várias vulnerabilidades em seu software QRadar Suite. Essas falhas, que afetam diversos componentes, foram corrigidas na versão mais recente do software.

No boletim divulgado informa que a suíte QRadar, juntamente com o software IBM Cloud Pak for Security, contém várias vulnerabilidades que podem ser exploradas por invasores.

As seguintes versões se encontram com estas vulnerabilidades:

- IBM Cloud Pak for Security: Versões 1.10.0.0 a 1.10.11.0
- Software QRadar Suite: Versões 1.10.12.0 a 1.10.23.0

De acordo com o relatório da IBM, essas vulnerabilidades variam desde negação de serviço e cross-site scripting até manuseio inadequado de dados confidenciais e possível execução de código arbitrário. Abaixo estão as descrições detalhadas e as especificações técnicas de cada vulnerabilidade identificada:

Modulo jose no Node.js (CVE-2024-28176): Esta vulnerabilidade foi classificada pelo GitHub com a pontuação CVSS3.1: 4.9 de nível média, possuindo a seguinte descrição: “Jose é um módulo JavaScript para assinatura e criptografia de objetos JSON, fornecendo suporte para JSON Web Tokens (JWT), JSON Web Signature (JWS), JSON Web Encryption (JWE), JSON Web Key (JWK), JSON Web Key Set (JWKS) e muito mais. Uma vulnerabilidade foi identificada nas interfaces de descriptografia JSON Web Encryption (JWE), especificamente relacionadas ao suporte para descompactação de texto simples após sua descriptografia. Sob certas condições, é possível que o ambiente do usuário consuma uma quantidade excessiva de tempo de CPU ou memória durante as operações de descriptografia JWE. Esse problema foi corrigido nas versões 2.0.7 e 4.15.5”. Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Jinja Cross-Site Scripting (CVE-2024-34064): Esta vulnerabilidade foi classificada pelo GitHub com a pontuação CVSS3.1: 5.4 de nível média, possuindo a seguinte descrição: “Jinja é um mecanismo de modelagem extensível. O filtro 'xmlattr' nas versões afetadas do Jinja aceita chaves contendo caracteres que não são de atributo. Os atributos XML/HTML não podem conter espaços, '/', '>' ou '=', pois cada um seria interpretado como iniciando um atributo separado. Se um aplicativo aceitar chaves (em vez de apenas valores) como entrada do usuário e renderizá-las em páginas que outros usuários também veem, um invasor poderá usar isso para injetar outros atributos e executar

XSS. A correção para CVE-2024-22195 abordou apenas espaços, mas não outros caracteres. Aceitar chaves como entrada do usuário agora é explicitamente considerado um caso de uso não intencional do filtro 'xmlattr', e o código que faz isso sem validar a entrada deve ser sinalizado como inseguro, independentemente da versão do Jinja. Aceitar valores como entrada do usuário continua sendo seguro. Esta vulnerabilidade foi corrigida na versão 3.1.4." Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Negação de serviço no módulo idna (CVE-2024-3651): Esta vulnerabilidade foi classificada pelo NIST com a pontuação CVSS3.1: 7.5 de nível alta, possuindo a seguinte descrição: "Foi identificada uma vulnerabilidade na biblioteca kjd/idna, especificamente na função 'idna.encode()', afetando a versão 3.6. O problema surge do tratamento da função de cadeias de caracteres de entrada criadas, o que pode levar a uma complexidade quadrática e, consequentemente, a uma condição de negação de serviço. Essa vulnerabilidade é acionada por uma entrada criada que faz com que a função 'idna.encode()' processe a entrada com carga computacional considerável, aumentando significativamente o tempo de processamento de maneira quadrática em relação ao tamanho da entrada."

Armazenamento de credenciais em texto claro (CVE-2024-25024): Esta vulnerabilidade foi classificada pela NIST com a pontuação CVSS 3.1: 5.5 de nível média, possuindo a seguinte descrição: "O IBM QRadar Suite Software 1.10.12.0 a 1.10.23.0 e o IBM Cloud Pak for Security 1.10.0.0 a 1.10.11.0 armazenam credenciais do usuário em texto simples e claro que pode ser lido por um usuário local. ID do IBM X-Force: 281430."

Negação de serviço gRPC em Node.js (CVE-2024-37168): Esta vulnerabilidade foi classificada pelo GitHub com pontuação CVSS3.1: 5.3 de nível médio, possuindo a seguinte descrição: "@grpc/grps-js implementa a funcionalidade principal do gRPC puramente em JavaScript, sem um complemento C++. Antes das versões 1.10.9, 1.9.15 e 1.8.22, há dois caminhos de código separados nos quais a memória pode ser alocada por mensagem além da opção de canal 'grpc.max_receive_message_length': Se uma mensagem recebida tiver um tamanho na conexão maior que o limite configurado, toda a mensagem será armazenada em buffer antes de ser descartada; e/ou se uma mensagem recebida tiver um tamanho dentro do limite na transmissão, mas for descompactada para um tamanho maior que o limite, toda a mensagem será descompactada na memória e no servidor não será descartada. Isso foi corrigido nas versões 1.10.9, 1.9.15 e 1.8.22." Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Divulgação de informações no Node.js undici (CVE-2024-30260): Esta vulnerabilidade foi classificada pelo GitHub com pontuação CVSS3.1: 3.9 de nível baixo, possuindo a seguinte descrição: "Undici é um cliente HTTP/1.1, escrito do zero para Node.js. Undici limpou os cabeçalhos Authorization e Proxy-Authorization para 'fetch()', mas não os limpou para 'undici.request()'. Esta vulnerabilidade foi corrigida na(s) versão(ões) 5.28.4 e 6.11.1". Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Bypass de segurança Node.js (CVE-2024-30261): Esta vulnerabilidade foi classificada pelo GitHub com pontuação CVSS3.1: 2.6 de nível baixo, possuindo a seguinte descrição: "Undici é um cliente HTTP/1.1, escrito do zero para Node.js. Um invasor pode alterar a opção 'integrity' passada para 'fetch()', permitindo que 'fetch()' aceite solicitações como válidas, mesmo que tenham sido adulteradas. Esta vulnerabilidade foi corrigida na(s) versão(ões) 5.28.4 e 6.11.1". Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Exibição inadequada de dados (CVE-2024-28799): Esta vulnerabilidade foi classificada pela IBM Corporation com pontuação CVSS3.1: 5.6 de nível médio, possuindo a seguinte descrição: "O IBM QRadar Suite Software 1.10.12.0 a 1.10.23.0 e o IBM Cloud Pak for Security 1.10.0.0 a

1.10.11.0 exibem dados sensíveis incorretamente durante comandos de backend, o que pode resultar na divulgação inesperada dessas informações. ID do IBM X-Force: 287173". Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Execução de código arbitrário em loops rápidos (CVE-2024-39008): Esta vulnerabilidade foi classificada pelo CISA-ADP com pontuação CVSS3.1: 10.0 de nível crítico, possuindo a seguinte descrição: "descobriu-se que o robinweser fast-loops v1.1.3 contém um protótipo de poluição por meio da função objectMergeDeep. Essa vulnerabilidade permite que invasores executem código arbitrário ou causem uma negação de serviço (DoS) por meio da injeção de propriedades arbitrárias". Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Node.js Módulo ip SSRF (CVE-2024-29415): Esta vulnerabilidade foi classificada pelo CISA-ADP com pontuação CVSS3.1: 8.1 de nível alto, possuindo a seguinte descrição: "O pacote ip por meio de 2.0.1 para Node.js pode permitir SSRF porque alguns endereços IP (como 127.1, 01200034567, 012.1.2.3, 000:0:0000::01 e ::fFFf:127.0.0.1) são categorizados incorretamente como globalmente roteáveis por meio de isPublic. NOTA: esse problema existe devido a uma correção incompleta para CVE-2023-42282." Esta vulnerabilidade ainda aguarda análise de classificação pela NIST.

Mitigação e Prevenção:

A IBM recomenda fortemente que os usuários façam upgrade para a versão 1.10.24.0 ou posterior. No momento, nenhuma solução alternativa ou mitigação está disponível. Os usuários são incentivados a aplicar as atualizações imediatamente.

Mitigação e prevenção com Qualys e Trend Micro:

Qualys:

- Realize uma varredura completa em todos os sistemas para identificar a presença das vulnerabilidades do IBM QRadar. Utilize os relatórios detalhados para entender a extensão das falhas e priorizar os sistemas que necessitam de atenção imediata.
- Automatize a aplicação de patches nos sistemas afetados. Certifique-se de que os patches específicos para as vulnerabilidades do IBM QRadar sejam aplicados em todos os sistemas identificados.
- Configure o monitoramento contínuo para detectar qualquer nova instância das vulnerabilidades e garantir que todos os sistemas permaneçam protegidos.

Trend Micro

- Utilize a detecção e resposta estendidas (XDR) para identificar atividades suspeitas relacionadas à exploração das vulnerabilidades. Isso inclui monitorar tráfego de rede, endpoints, servidores e e-mails.
- Aplique a análise de comportamento para detectar padrões anômalos que possam indicar tentativas de exploração das vulnerabilidades.
- Implemente a proteção de endpoints para bloquear tentativas de execução de código malicioso que possam explorar as vulnerabilidades. Certifique-se de que todos os endpoints estejam atualizados com as últimas definições de segurança.

- Utilize as capacidades de resposta a incidentes para isolar e remediar sistemas comprometidos rapidamente. Isso inclui a quarentena de arquivos maliciosos e a interrupção de conexões de rede suspeitas.
- Realize campanhas de conscientização e treinamento para os usuários finais sobre a importância de aplicar patches e reconhecer sinais de possíveis ataques.
- Mantenha backups regulares e testados de todos os sistemas críticos para garantir a recuperação rápida em caso de comprometimento.
- Reforce as políticas de segurança, incluindo a aplicação de patches regulares e a revisão contínua das configurações de segurança.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/ibm-qradar-vulnerabilities/ , https://www.ibm.com/support/pages/node/7165488 e https://nvd.nist.gov/

2.2. Vulnerabilidade RCE do Windows Secure Channel permite que invasores injetem arquivos maliciosos remotamente.

O Windows Secure Channel, é um componente vital para a gestão de comunicações seguras na Internet, ele está atualmente sob intensa análise devido a uma vulnerabilidade recém-descoberta de execução remota de código (RCE). Se explorada, essa falha pode permitir que invasores executem código arbitrário nos sistemas afetados, concedendo-lhes controle total sobre a máquina alvo.

Esta vulnerabilidade recebeu a identificação: CVE-2024-38148 sendo classificada de acordo com a Microsoft com a pontuação CVSS v3.1: 7.5 de nível alto e está descrita como: “Vulnerabilidade de Negação de Serviço no Canal Seguro do Windows” a vulnerabilidade não foi classificada pela NIST. Inicialmente acabou sendo identificada como um problema de integer overflow. No entanto, uma investigação mais aprofundada determinou que se tratava de Use-After-Free (UAF). Esse tipo de vulnerabilidade ocorre quando um programa continua usando um ponteiro após a liberação da memória a que ele faz referência, levando a um comportamento imprevisível e a uma possível exploração.

Exploração

Segundo o relatório, essa vulnerabilidade pode ser explorada por invasores para injetar arquivos maliciosos em canais de comunicação seguros, sem que a vítima perceba. Esses arquivos podem incluir desde malware e ransomware até ferramentas avançadas de espionagem, projetadas para roubar dados confidenciais ou interromper operações. O perigo está na natureza furtiva desse vetor de ataque as vítimas podem não perceber que seus sistemas foram comprometidos até que seja tarde demais. Sendo detectada na função: CSsl3TlsContext::CSsl3TlsContext.

A Microsoft lançou um patch que introduziu uma verificação condicional para evitar uma operação de atribuição insegura.

```
if ( !(unsigned
__int8)wil::details::FeatureImpl<__WilFeatureTraits_Feature_261269
6381>::__private_IsEnabled(&`wil::Feature<__WilFeatureTraits_Featu
re_2612696381>::GetImpl'::`2'::impl) )
{
  *(_QWORD *)(this + 472) = *(_QWORD *)(a2 + 472);
  *(_QWORD *)(a2 + 472) = 0i64;
}
```

Figura 1 – Patch de verificação condicional. Fonte: https://cybersecuritynews.com/windows-secure-channel-vulnerability/

Este patch bloqueou efetivamente a operação de atribuição de um campo específico quando um determinado recurso foi habilitado.

Usando o IDA para análise binária, foi descoberto que uma nova alocação de memória (denominada M1) foi atribuída ao campo no deslocamento 472 (hex: 1D8h) dentro da função. Verificou-se que a função atribui um ponteiro a essa memória recém-alocada, o que pode levar a um possível cenário de uso após liberação (UAF).

A função em questão é a: CSsl3TlsServerContext::ProcessRecordCTlsMessageFragment::Initialize.

```
void __fastcall CTlsMessageFragment::Initialize(CTlsMessageFragment
*this, struct CSsl3TlsContext *a2)
{
  int v2; // eax
  int v3; // edx
  unsigned int v4; // edx
  unsigned int v5; // eax

  *(_QWORD *)this = a2;
  ......
  v3 = 1536;
LABEL_9:
  *((_DWORD *)this + 3) = v3;
  v5 = *((_DWORD *)this + 2);
  if ( v5 > 0xFFFFFF )
    v5 = 0xFFFFFF;
  *((_DWORD *)this + 2) = v5;
}
```

Figura 2 – IDA Análise Binária. Fonte: https://cybersecuritynews.com/windows-secure-channel-vulnerability/

A análise revelou que, embora o patch tenha definido o 472º campo da estrutura como zero, o primeiro campo de M1 não foi atualizado. Esse descuido permitiu que o primeiro campo de M1 continuasse apontando para a memória anterior, criando uma vulnerabilidade de uso após liberação (UAF) durante o processo de lançamento.

Segundo afirmações de pesquisadores, após testes práticos, confirmou-se que há, de fato, um problema de UAF neste local. A partir do ponto de uso, pode-se perceber que ele utilizará a tabela virtual da estrutura. Se a posição estiver ocupada corretamente, a falha pode ser explorada diretamente. Com gadgets adequados, a execução remota de código pode ser alcançada.

O potencial de dano dessa vulnerabilidade é significativo. Se explorada corretamente, pode permitir a execução remota de código não autenticado. Isso significa que um invasor pode executar código arbitrário em um sistema remoto sem a necessidade de autenticação prévia, representando um grave risco à segurança.

Mitigação

Esta vulnerabilidade se encontra corrigida no patch tuesday lançado em 13 de agosto de 2024, as respectivas identificações das atualizações podem ser conferidas conforme imagem abaixo:

Product	Article
Windows Server 2022, 23H2 Edition (Server Core installation)	5041573
Windows 11 Version 23H2 for x64-based Systems	5041585
Windows 11 Version 23H2 for ARM64-based Systems	5041585
Windows 11 Version 22H2 for x64-based Systems	5041585
Windows 11 Version 22H2 for ARM64-based Systems	5041585
Windows 11 version 21H2 for ARM64-based Systems	5041592
Windows 11 version 21H2 for x64-based Systems	5041592
Windows Server 2022 (Server Core installation)	5041160
Windows Server 2022	5041160
Windows 11 Version 24H2 for x64-based Systems	5041571
Windows 11 Version 24H2 for ARM64-based Systems	5041571

Figura 3 – Versões do Windows e a identificação das KBs. Fonte: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148

Embora já tenha sido corrigida, o problema de Use-After-Free (UAF) serve como um lembrete das complexidades envolvidas na segurança de software. Isso também destaca a necessidade de vigilância contínua e de uma análise detalhada dos patches de segurança para garantir que todas as vulnerabilidades potenciais sejam devidamente abordadas.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38148 , https://cybersecuritynews.com/windows-secure-channel-vulnerability/ e https://nvd.nist.gov/vuln/detail/CVE-2024-38148

2.3. Vulnerabilidade no kernel do linux permite a elevação de privilégio local.

O kernel do Linux é o núcleo do sistema operacional, responsável por gerenciar recursos e permitir a execução de programas. Uma nova vulnerabilidade crítica foi identificada no kernel do Linux, permitindo que invasores locais executem uma elevação de privilégio. Esta vulnerabilidade recebeu a identificação: CVE-2024-43856 sendo classificada de acordo com a NIST com a pontuação CVSS v3.1: 5.5 de nível médio e está descrita como: “No kernel do Linux, a seguinte vulnerabilidade foi resolvida: dma: correção na ordem de chamadas em dmam_free_coherent A função dmam_free_coherent() libera uma alocação de DMA, tornando o endereço virtual (vaddr) liberado disponível para reutilização, e então chama devres_destroy() para remover e liberar a estrutura de dados usada para rastrear a alocação de DMA. Entre essas duas chamadas, é possível que uma tarefa concorrente faça uma alocação com o mesmo vaddr e a adicione à lista devres. Se isso acontecer, haverá duas entradas na lista devres com o mesmo vaddr, e devres_destroy() pode liberar a entrada errada, acionando o WARN_ON() em dmam_match. A correção foi feita destruindo a entrada devres antes de liberar a alocação de DMA”.

A vulnerabilidade identificada reside na função map_write do subsistema de mapeamento de memória (Memory Mapping Subsystem). Essa função possui uma falha que permite que um usuário local com privilégios baixos manipule o mapeamento de memória para executar código com permissões elevadas.

Se explorada com sucesso, essa falha pode permitir que invasores comprometam sistemas inteiros, desde a manipulação de arquivos de sistema até a instalação de malware persistente.

Exploração

A exploração desta vulnerabilidade exige que o invasor tenha acesso local ao sistema-alvo. No entanto, a necessidade de acesso local não diminui a gravidade da falha, especialmente em ambientes onde múltiplos usuários compartilham acesso a servidores ou em configurações onde a segurança interna é uma preocupação.

Um cenário comum de exploração envolve o seguinte:

1. Obtenção de Acesso Local: O invasor inicialmente obtém acesso a uma conta de usuário com privilégios limitados no sistema.
2. Manipulação da Memória: Usando a falha na função map_write, o invasor modifica os mapeamentos de memória do sistema, conseguindo acesso a áreas de memória críticas.
3. Injeção de Código Malicioso: O invasor então injeta código malicioso na memória, que é executado com privilégios de kernel. Isso pode incluir comandos para adicionar novos usuários com privilégios de root, alterar configurações críticas do sistema, ou instalar backdoors para acesso futuro.

Essa exploração pode ser difícil de detectar em tempo real, pois o código malicioso é executado no nível do kernel, o que significa que pode desativar ou ignorar mecanismos de segurança convencionais.

Mitigação e prevenção

A vulnerabilidade foi corrigida nas versões mais recentes do kernel do Linux. As seguintes versões do kernel contêm as correções necessárias:

- Kernel Linux 6.5.3 e superiores: As versões a partir do 6.5.3 incluem uma correção completa para a vulnerabilidade CVE-2023-42793. Administradores devem atualizar seus sistemas para pelo menos esta versão ou superior para garantir a segurança;
- Kernel Linux 6.1.54 (LTS) e superiores: Para sistemas que utilizam versões de Long Term Support (LTS), a versão 6.1.54 inclui a correção e deve ser aplicada imediatamente;
- Kernel Linux 5.15.131 (LTS) e superiores: A versão 5.15.131, também LTS, inclui a correção e deve ser aplicada em ambientes que dependem dessa versão para suporte a longo prazo;
- Kernel Linux 4.19.297 (LTS) e superiores: Sistemas legados que operam na versão 4.19 do kernel devem ser atualizados para a versão 4.19.297 ou posterior, onde a falha foi corrigida.

Os administradores devem verificar a versão do kernel em execução e atualizar para as versões mencionadas acima. Essa atualização é crítica para evitar a exploração da vulnerabilidade.

Antes de realizar a atualização em ambientes de produção, é recomendável testar a nova versão do kernel em um ambiente de teste para garantir a compatibilidade com aplicações e sistemas dependentes.

Após a atualização, revise as configurações do sistema para garantir que todas as políticas de segurança estejam alinhadas com as melhores práticas. Isso inclui a revisão de permissões de usuários, controles de acesso e auditoria de logs para identificar qualquer atividade suspeita anterior à atualização.

Implemente sistemas de monitoramento para detectar tentativas de exploração e garantir que os sistemas permaneçam protegidos após a aplicação do patch.

Mitigação e prevenção com Qualys e Trend Micro

Qualys:

- Utilize o Qualys Vulnerability Management (VM) para realizar varreduras detalhadas em todos os sistemas baseados em Linux na sua rede.
- Identifique instâncias do kernel do Linux que são vulneráveis a essa falha específica usando as assinaturas de vulnerabilidades do Qualys.
- Priorize a correção das instâncias vulneráveis utilizando a funcionalidade de priorização de ameaças do Qualys, focando em sistemas críticos e servidores de produção.
- Aplique patches de segurança e atualizações do kernel fornecidos pelas distribuições Linux afetadas o mais rápido possível.
- Utilize o Qualys Patch Management para automatizar o processo de aplicação de patches, garantindo que todas as correções sejam distribuídas e aplicadas de maneira eficiente em toda a rede.
- Ative o monitoramento contínuo com o Qualys para detectar novas vulnerabilidades em tempo real, assegurando que a infraestrutura de TI esteja sempre protegida contra ameaças emergentes.
- Configure alertas automáticos para qualquer atividade suspeita ou mudanças relacionadas ao kernel do Linux nos sistemas monitorados.

Trend Micro:

- Utilize o Trend Micro Vision One para proteger seus sistemas Linux contra a exploração dessa vulnerabilidade, aplicando políticas de proteção contra exploits conhecidos.
- Configure regras de prevenção de intrusão (IPS) específicas para detectar e bloquear tentativas de exploração dessa falha no kernel do Linux.
- Utilize a análise de comportamento do Trend Micro Vision One para identificar atividades suspeitas, como tentativas de elevação de privilégios ou execução de código anômalo.
- Monitore logs e eventos de segurança para detectar padrões de ataque relacionados a essa vulnerabilidade no kernel do Linux.
- Integre o Trend Micro Vision One com a equipe de resposta a incidentes para facilitar uma resposta rápida e coordenada a qualquer tentativa de exploração detectada.
- Utilize playbooks de resposta automática para isolar sistemas comprometidos e restaurar rapidamente as operações normais, minimizando o impacto das explorações.
- Fortaleça as configurações de segurança nos sistemas Linux, implementando controles rigorosos de acesso e práticas recomendadas de segurança, como a desativação de serviços não necessários.

- Realize auditorias regulares de segurança utilizando o Trend Micro Vision One para garantir que as políticas de segurança estejam sendo seguidas e que não existam configurações inseguras.
- Eduque os administradores de sistemas sobre as práticas recomendadas para o gerenciamento de patches e a importância de manter o kernel atualizado.
- Ofereça treinamentos regulares para a equipe de segurança sobre como identificar e responder a incidentes relacionados a essa vulnerabilidade.

Para ver mais detalhes sobre esta vulnerabilidade você pode acessar os endereços a seguir: https://cybersecuritynews.com/linux-kernal-vulnerability/ e https://nvd.nist.gov/vuln/detail/CVE-2024-43856

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