CVE

(VULNERABILIDADES E EXPOSIÇÕES COMUNS)

AUTOR: JOÃO PEDRO DA CUNHA CAIXETA

DATA: 06/12/2024

ÍNDICE

01.

Introdução

02.

Desenvolvimento

03.

INTRODUÇÃO

Objetivo

O objetivo deste relatório é explorar o conceito de Common Vulnerabilities and Exposures (CVE), destacando sua importância no contexto da segurança cibernética. Serão abordados os benefícios de sua padronização, a estrutura de identificação das vulnerabilidades, bem como os principais desafios enfrentados pelas organizações na mitigação de riscos associados a essas exposições.

Escopo

Este relatório cobre:

1. **Definição e Funcionamento:** Uma explicação detalhada sobre o que é o CVE e como ele opera no cenário global.
2. **Importância do CVE:** O papel do CVE como ferramenta essencial para identificar e categorizar vulnerabilidades de segurança.
3. **Estrutura e Funcionamento:** Uma análise de como as vulnerabilidades são catalogadas e distribuídas por meio do sistema CVE.
4. **Estudos de Caso:** Exemplos práticos de uso do CVE em organizações e na resposta a incidentes.
5. **Desafios e Recomendações:** Reflexões sobre os principais desafios associados ao uso do CVE e sugestões para aprimorar sua adoção.

O relatório foca nas vulnerabilidades em sistemas, aplicações e dispositivos de rede, excluindo análises detalhadas sobre ferramentas específicas de mitigação.

Contextualização

Em um mundo cada vez mais conectado, a segurança cibernética se tornou uma prioridade para empresas, governos e usuários individuais. As ameaças evoluem constantemente, tornando fundamental a existência de mecanismos padronizados para identificar, categorizar e comunicar vulnerabilidades em sistemas.

O Common Vulnerabilities and Exposures (CVE), criado em 1999 pelo MITRE Corporation, é uma das ferramentas mais amplamente utilizadas para esse fim. Ele fornece um identificador único para vulnerabilidades conhecidas, facilitando a comunicação entre desenvolvedores, analistas de segurança e organizações. Por meio da adoção do CVE, empresas podem priorizar correções, reduzir riscos e melhorar a postura de segurança de suas infraestruturas.

Entender o funcionamento e a aplicabilidade do CVE é crucial para profissionais de TI e cibersegurança que buscam soluções eficazes para um ambiente digital mais seguro.

CVE - Figura 1

DESENVOLVIMENTO

Definição

Common Vulnerabilities and Exposures (CVE) é um banco de dados que registra vulnerabilidades e fraquezas relacionadas a segurança da informação conhecidas publicamente. A missão do programa é identificar, definir e catalogar as vulnerabilidades a fim de facilitar o compartilhamento de informações.

História

O sistema foi lançado oficialmente para o público em setembro de 1999, operado pela *MITRE Corporation,* financiado pelo Departamento de Segurança Interno dos Estados Unidos e mantido pela *National Cybersecurity FFRDC* (NCF), um centro de pesquisa e desenvolvimento.

Vulnerabilidades x Exposições

O programa CVE define uma vulnerabilidade como "uma fraqueza na lógica computacional encontrada em componentes de software e hardware que, quando explorada, resulta em um impacto negativo na confidencialidade, integridade ou disponibilidade". Portanto, uma vulnerabilidade se refere a uma fraqueza, como um erro de programação, que pode ser usada por invasores para obter acesso não autorizado a redes e sistemas, instalar malware, executar código e roubar ou destruir dados confidenciais. Uma exposição permite esse acesso.

Pense em uma casa: uma vulnerabilidade é uma janela com uma fechadura que é fácil de ser arrombada por um ladrão. Uma exposição é uma janela que alguém esqueceu de trancar.

O que se qualifica como um CVE?

Para se qualificar como um CVE e receber um identificador CVE (ID CVE), uma falha de segurança deve atender a determinados critérios:

- Corrigível independente de outras falhas: a falha deve poder ser corrigida separadamente de outras vulnerabilidades.
- Reconhecida pelo fornecedor ou documentado em um relatório de vulnerabilidades: o fornecedor deve reconhecer que o bug existe e afeta negativamente a segurança. Ou deve haver um relatório de vulnerabilidades que demonstre o impacto negativo do bug na segurança e sua violação da política de segurança do sistema afetado.
- Afeta uma base de código: o bug deve afetar apenas uma base de código (um produto). As falhas que afetam mais de um produto são atribuídas a CVEs separados para cada produto.

CNAs

As autoridades de numeração CVE (CNAs) atribuem IDs CVE e publicam registros CVE dentro de escopos de cobertura específicos. A empresa MITRE funciona como editor e CNA primário. Outras CNAs incluem os principais fornecedores de sistemas operacionais (SO) e TI (incluindo IBM, Microsoft e Oracle), pesquisadores de segurança e outras entidades autorizadas. As CNAs operam de forma voluntária. Atualmente, existem 389 CNAs de 40 países diferentes.

No Brasil existem CNAs, como por exemplo a Sophos, QNAP e Red Hat Security, que é uma das principais colaboradoras do software open source.

Raízes e raízes de nível superior

Raízes são organizações autorizadas a recrutar, treinar e governar CNAs ou outras raízes dentro de um escopo específico.

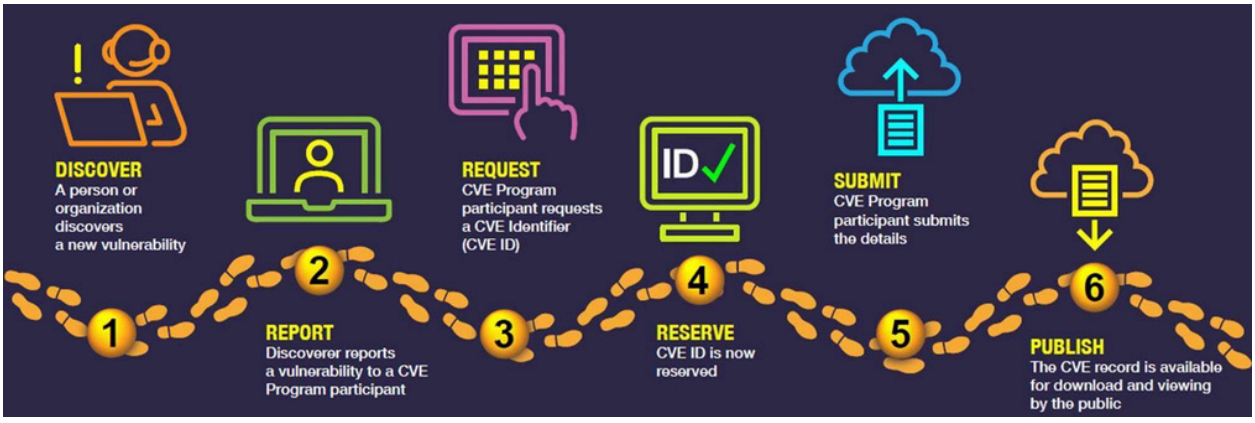
Raízes de nível superior são as raízes de nível mais alto e são responsáveis pela "governança e administração de uma hierarquia específica, incluindo raízes e CNAs dentro dessa hierarquia."5 Atualmente, há duas raízes de nível superior no programa CVE: a MITRE Corporation e a Cybersecurity and Infrastructure Security Agency (CISA).

Ciclo de Vida de Registro CVE

Atualmente existem um total de **240.830** vulnerabilidades identificadas, registradas, categorizadas e publicadas no banco de dados nacional de vulnerabilidades da CISA (Cybersecurity and Infrastructure Security Agency) - e o número só continua a crescer.

Muitas empresas oferecem uma recompensa por bugs — uma recompensa por encontrar e relatar com responsabilidade vulnerabilidades encontradas no software.

Mas afinal, como funciona o processo de registro de CVE?



CVE Lifecycle Register - Figura 2

1. Uma pessoa ou organização descobre através de testes uma nova vulnerabilidade.
2. Quem descobriu a vulnerabilidade relata a um parceiro do Programa CVE.
3. O parceiro do Programa CVE atribui um identificador (ID) que é único e alfanumérico. Cada ID faz referência a uma vulnerabilidade específica.
4. O ID, que é a parte inicial de um registro CVE, é reservado. O estado Reservado significa que as partes interessadas do CVE estão usando o ID do CVE para coordenação e gerenciamento de vulnerabilidade em estágio inicial, mas a Autoridade de Numeração CVE ainda não está pronta para divulgar publicamente a vulnerabilidade.
5. O parceiro do Programa CVE envia os detalhes e incluem, entre outros, os produtos afetados; versões de produtos afetados ou corrigidas; tipo de vulnerabilidade, causa raiz ou impacto; e pelo menos uma referência pública.
6. Uma vez incluídos os elementos de dados mínimos exigidos no Registro CVE, ele é Publicado na Lista CVE pelo CNA responsável.

Estrutura

CVE Structure - Figura 3

Como mostrado na Figura 3, a estrutura é composta pelo prefixo "CVE", seguido pelo ano da publicação da vulnerabilidade (não indica quando a vulnerabilidade foi descoberta) e com o ID final, que podem incluir quatro ou mais dígitos, sem limitar o número de dígitos arbitrários.

Como mostrado na Figura 3, a estrutura é composta pelo prefixo "CVE", seguido pelo ano da publicação da vulnerabilidade (não indica quando a vulnerabilidade foi descoberta) e com o ID final, que podem incluir quatro ou mais dígitos, sem limitar o número de dígitos arbitrários.

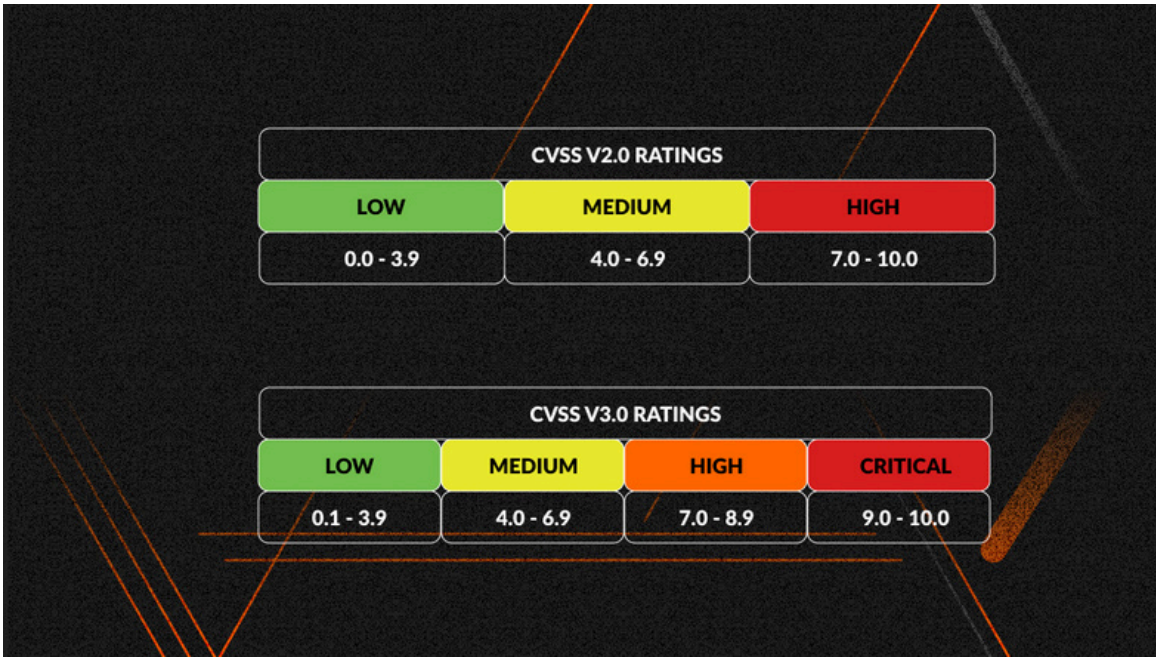
Existem algumas regras impostas pela Autoridade de Numeração CVE para a atribuição de ID, como por exemplo:

- Divulgar publicamente e atribuir um ID CVE se a vulnerabilidade tem o potencial de causar danos significativos ou requer ação ou avaliação de risco por partes que não sejam a CNA ou o Fornecedor.
- Os CNAs NÃO DEVEM considerar o tipo de tecnologia (por exemplo, nuvem, local, inteligência artificial, aprendizado de máquina) como a única base para determinar a atribuição.
- CNAs DEVEM atribuir IDs CVE independentemente de uma Correção estar disponível ou não.
- Os CNAs NÃO DEVEM atribuir IDs CVE a vulnerabilidades em produtos que não estão e nunca estiveram disponíveis publicamente.

CVSS

Uma maneira de as organizações avaliarem a gravidade das vulnerabilidades é usando o Sistema de Pontuação de Vulnerabilidades Comuns (CVSS). O CVSS - operado pelo Fórum de Equipes de Resposta a Incidentes e Segurança (FIRST) - é um método padronizado usado pelo Banco de Dados Nacional de Vulnerabilidades (NVD), Equipes de Resposta a Emergências de Cibersegurança (CERTs) e outros para avaliar a gravidade e o impacto das vulnerabilidades relatadas. É separado do sistema CVE, mas usado junto com o CVE: os formatos de registro CVE permitem que as CNAs adicionem uma pontuação CVSS aos registros CVE ao publicar registros na lista CVE. O NVD fornece enriquecimento CVSS para todos os registros CVE publicados.

O CVSS atribui uma pontuação numérica às vulnerabilidades, variando de 0.0 a 10, com base na explorabilidade, escopo de impacto e outras métricas. Quanto maior a pontuação, mais grave é o problema. Essa pontuação ajuda as organizações a avaliar a urgência de lidar com uma vulnerabilidade específica e alocar recursos adequadamente. Não é incomum que organizações também usem seu próprio sistema de pontuação de vulnerabilidades.



CVSS Table - Figura 4

O CVSS V2.0 e o CVSS V3.0 consistem em três grupos de métricas:

- **Base:** Avalia a severidade intrínseca de uma vulnerabilidade, por exemplo o impacto e facilidade de exploração.
- **Temporal:** Considera fatores que mudam ao longo do tempo, como a disponibilidade de patches.
- **Ambiental:** Ajusta a pontuação com base no ambiente específico do usuário.

V2.0 foi criado em 2007 e havia falta de clareza e flexibilidade ao refletir o impacto real em cenários modernos, então logo foi criado o V3.0 em 2015 que buscou apresentar melhorias mais refinadas nas métricas para representar melhor cenários mais complexos. Além disso, houve também uma consideração de interdependência de sistemas.

O **CVSS V4.0** é um pouco diferente e acrescenta um 4º grupo de métrica: Suplementar, que ajuda a adaptar análise do CVSS ao contexto de segurança em evolução, levando em conta fatores mais subjetivos ou contextuais que as métricas padrão não podem capturar. Foi lançado em 2023 e houveram vários avanços comparado ao V3.0, como por exemplo:

- Métricas mais expandidas, que oferecem uma visão mais dinâmica da criticidade da vulnerabilidade.
- Perfis adaptáveis que permite que organizações criem perfis personalizados para adaptar o CVSS ao contexto de suas operações.
- Maior granularidade e contextualização.
- Melhor alinhamento com ambientes modernos (nuvem, IoT, etc.)

Característica	CVSS V2.0	CVSS V3.0	CVSS V4.0
Métricas	Simples	Ajustáveis	Enriquecidas
Exploits e Impacto	Básico	Detalhado	Mais Granular
Escopo	Não Considerado	Detalhado	Refinado

Lista de CVEs

Mesmo as vulnerabilidades mais conhecidas continuam muito perigosas. Pode ser que já exista uma solução disponível, mas os usuários podem não tê-la aplicado com sucesso, se é que aplicaram. Os profissionais de segurança cibernética estão muito atentos a vários níveis de gravidade de milhares de vulnerabilidades. Mas como se manter sempre alerta? A lista abaixo destaca as vulnerabilidades mais preocupantes no momento, e sabemos que à medida que novas ameaças surgem, o resposta também será outra.

Exploit 1: Microsoft Exchange

CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, e CVE-2021-27065

Embora a Microsoft rapidamente tenha lançado pacotes para corrigir essas vulnerabilidades conhecidas como Dia Zero, este sempre será um dos tópicos de segurança cibernética popular nos noticiários. Mesmo após o lançamento e divulgação da correção, nas semanas seguintes, os ataques continuam a aumentar, o que significa que muitos usuários não implementam os pacotes de correção. CVE-2021-26855 pode permitir que um invasor tenha acesso às caixas de correio, enquanto CVE-2021-26857, CVE-2021-26858 e CVE-2021-27065 permitem a execução remota de código.

Exploit 2: Fortinet FortiGate SSL VPN

CVE-2018-13379, CVE-2020-12812, CVE-2019-5591

Vários avisos oficiais sobre essas vulnerabilidades foram enviados por agências governamentais, incluindo o National Cyber Security Center (NCSC) do Reino Unido, o Federal Bureau of Investigation (FBI) e a Cybersecurity and Infrastructure Security Agency (CISA). Segundo estes alertas, os atores da Advanced Persistent Threat (APT) e os criminosos cibernéticos procuravam e usavam essas vulnerabilidades para fins de espionagem cibernética contra serviços governamentais, bem como em ataques de ransomware (sequestro digital de equipamentos) contra empresas comerciais. Em novembro de 2020, os invasores publicaram uma lista de mais de 50.000 IPs que permaneciam sem a correção.

Exploit 3: Suíte de Colaboração Synacor Zimbra (XXE)

CVE-2019-9670

A Agência de Segurança Nacional, CISA e o FBI, alertaram que o Serviço de Inteligência Estrangeiro Russo (SVR) explorou em várias ocasiões cinco vulnerabilidades já conhecidas, visando redes Americanas e aliadas, incluindo segurança nacional e sistemas relacionados ao governo. Toda agência governamental, bem como pessoas com contratos governamentais, foram alertados a verificar se alguma dessas vulnerabilidades se aplica a seus ambientes de TI e, em caso afirmativo, a tomar medidas para reduzir ou eliminar essas vulnerabilidades.

O recurso de caixa de correio do Synacor Zimbra Collaboration Suite possui um XML Eternal Entity Injection que pode ser explorado para obter acesso às credenciais. Além de estar listado na declaração conjunta, ele também foi relatado em um comunicado anterior pela NCSC sobre vulnerabilidades sendo exploradas em ataques direcionados à pesquisa e desenvolvimento da vacina COVID-19. Foi lançado um pacote para corrigir esta vulnerabilidade.

Exploit 4: Pulse Secure Pulse Connect Secure VPN

CVE-2019-11510

Esta vulnerabilidade está entre as cinco vulnerabilidades exploradas pelo SVR – Serviço de Inteligência Estrangeiro Russo. Este Pulse VPN contém uma vulnerabilidade de passagem de caminho em certas versões que permite que atacantes remotos não autenticados acessem informações confidenciais. Apesar de um pacote de correção ter sido lançado em abril de 2019 – mesmo antes de um comunicado anterior da CISA em 2020, foi observado um amplo uso da exploração desta vulnerabilidade.

Exploit 5: Citrix Application Delivery Controller and Gateway

CVE-2019-19781

Esta vulnerabilidade – semelhante ao Pulse VPN , também estava sendo explorada pelo SVR – Serviço de Inteligência Estrangeiro Russo. Identificada como Dia Zero, ela permitiu que invasores não autenticados acessassem informações confidenciais e arquivos de configuração. Esta vulnerabilidade pode também ser usada para ataques *DoS, phishing* e execução remota de código. Mesmo sabendo que são alvos fáceis, 19% das 80.000 empresas afetadas ainda não fizeram as correções recomendadas meses depois – apesar de conhecidamente várias instâncias desse exploit serem usadas por agentes de ameaças.

Exploit 6: VMware Workspace ONE Access

CVE-2020-4006

Também explorada pelo SVR e aberta a invasores, esta vulnerabilidade de injeção de comando também estava na lista, e é usada para executar comandos em sistemas para acessar dados protegidos. A NSA alertou sobre a vulnerabilidade em dezembro de 2020 e aconselhou o fortalecimento das senhas, uma vez que a vulnerabilidade ainda exigia acesso autenticado para ser utilizada. Apesar de já haver um pacote de correção disponível e vinculado ao alerta, ele ainda não foi amplamente implementado, uma vez que a vulnerabilidade continua sendo usada ativamente em novos ataques.

Exploit 7: Microsoft SMBGhost

CVE-2020-0796

Essa vulnerabilidade de execução remota de código utiliza o protocolo Microsoft Server Message Block (SMB), que era o mesmo protocolo visado pelo ransomware WannaCry – isto a torna muito preocupante. Com danos estimados em mais de um bilhão de dólares em mais de 100 países, os especialistas em segurança cibernética querem fazer o que puderem para evitar que o WannaCry repita este incidente. Mesmo já corrigida há mais de um ano, essa vulnerabilidade continua existindo – apesar de toda a preocupação, e mais de 100.000 sistemas ainda não haviam sido atualizados até outubro de 2020.

Exploit 8: VMWare vCenter RCE

CVE-2021-21972

Semelhante à vulnerabilidade Citrix listada anteriormente, esta vulnerabilidade de execução remota de código é simples de explorar, já que qualquer usuário não autorizado pode tirar proveito dela. Apesar de postar correções rapidamente, muitos atores de ameaças já estavam postando Provas de Conceitos para explorar esta vulnerabilidade no Github, por isso é muito importante as organizações atualizarem seus sistemas que se encontram vulneráveis o mais rápido possível.

Exploit 9: Google Chrome Browser

CVE-2021-21193, CVE-2021-21206, CVE-2021-21220

Essas três vulnerabilidades foram diagnosticadas como ameaças de Dia Zero – (CVE-2021-21193) no mecanismo do navegador Chrome, Blink, que pode permitir que um atacante remoto explore a falha de heap. Os dois últimos (CVE-2021-21206, CVE-2021-21220) foram anunciados na mesma semana, podendo ambos ser usados para execução remota de código. Embora o Google tenha lançado rapidamente novas versões para corrigir essas vulnerabilidades, a preocupação real é que esta falha está se tornando um padrão de ameaças de Dia Zero. Com o uso em escala do Chrome, uma vulnerabilidade desta natureza pode causar danos em uma escala global. Alguns especialistas ficaram muito cautelosos com sua abordagem de segurança geral após a descoberta de três ameaças de Dia Zero em um período tão curto de tempo – os especialistas devem ficar de olho no navegador.

Exploit 10: Cisco AnyConnect Posture

CVE-2021-1366

Foram descobertas no canal de comunicação entre processos (IPC) do Cisco AnyConnect Secure Mobility Client para Windows, vulnerabilidades de controle de acesso impróprio e de caminho de pesquisa não controlado. podem permitir que Um usuário local autenticado pode elevar privilégios com essas vulnerabilidades e execute qualquer aplicativo na conta SYSTEM. A Cisco lançou Atualizações de software gratuitas foram lançadas pela Cisco para corrigir esta vulnerabilidade.

Desafios Associados ao CVE

A cada ano, o número de vulnerabilidades registradas cresce de forma acelerada, o que dificulta o acompanhamento e a priorização por equipes de segurança. Em 2023, mais de 25mil CVEs foram adicionados ao catálogo global, cobrindo diferentes plataformas, dispositivos e softwares. Empresas com equipes pequenas enfrentam dificuldades para revisar todos os relatórios e implementar soluções para cada vulnerabilidade.

Nem todas as vulnerabilidades têm o mesmo impacto. Algumas podem ser críticas, enquanto outras representam ameaças menores. A priorização requer análise cuidadosa. Vulnerabilidades críticas precisam ser corrigidas rapidamente, mas a aplicação de patches em sistemas operacionais, redes ou aplicativos pode demandar muito tempo e planejamento.

Ferramentas robustas de gestão de vulnerabilidades muitas vezes são caras, dificultando sua aquisição por pequenas empresas. Além que muitas organizações ainda gerenciam vulnerabilidades manualmente, o que aumenta o risco de erros humanos e atrasos.

Profissionais de TI e segurança que não entendem como interpretar e aplicar informações do CVE podem ignorar vulnerabilidades críticas. Equipes precisam ser treinadas para interpretar o CVSS, identificar vulnerabilidades relevantes e implementarem correções eficazes.

Ferramentas que Utilizam CVE

1. **Sistemas de Escaneamento de Vulnerabilidades**

   - **Nessus:** Detecta vulnerabilidades baseadas em CVE, apresentando relatórios detalhados com recomendações de mitigação.
   - **Qualys:** Solução em nuvem para escanear, priorizar e corrigir vulnerabilidades de acordo com o banco de dados CVE.
   - **OpenVAS:** Uma ferramenta de código aberto que identifica vulnerabilidades e mapeia CVEs correspondentes.
   - **Rapid7 InsightVM:** Integra CVEs ao gerenciamento de vulnerabilidades e prioriza com base no impacto.

Ferramentas que utilizam CVE- Figura 5

CONCLUSÃO

O sistema Common Vulnerabilities and Exposures (CVE) desempenha um papel crucial no fortalecimento da segurança cibernética global. Ele fornece uma estrutura padronizada para identificar, categorizar e comunicar vulnerabilidades em sistemas e softwares, facilitando a colaboração entre desenvolvedores, analistas de segurança e organizações.

Apesar de seus inúmeros benefícios, o uso eficiente do CVE apresenta desafios significativos, como o crescente volume de vulnerabilidades, a dificuldade de priorização de correções e a dependência de ferramentas especializadas. Superar esses obstáculos exige investimento em automação, treinamento contínuo e integração de práticas de gestão de vulnerabilidades nos processos de segurança.

As ferramentas e sistemas que incorporam o CVE, como escâneres de vulnerabilidades, soluções de patch management e plataformas SIEM, demonstram que a automação pode ser uma poderosa aliada na redução de riscos. Além disso, a adoção do CVE é essencial para atender a requisitos de conformidade regulatória e proteger organizações contra ameaças cibernéticas em constante evolução.

Portanto, compreender e aplicar o CVE de maneira estratégica não é apenas uma boa prática, mas uma necessidade para qualquer organização que busca manter a integridade, a confidencialidade e a disponibilidade de suas operações no ambiente digital. Este relatório destaca que, ao adotar o CVE como parte de um programa abrangente de segurança, empresas podem não apenas mitigar riscos, mas também fortalecer sua postura frente aos desafios do ciberespaço moderno.

REFERÊNCIAS

- https://pt.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
- https://cve.mitre.org/
- https://panorays.com/blog/what-is-cve/
- https://www.ibm.com/br-pt/think/topics/cve#:~:text=Para%20se%20qualificar%20como%20um,corrigida%20separadamente%20de%20outras%20vulnerabilidades.
- https://www.cve.org/about/Process
- https://www.cve.org/ResourcesSupport/AllResources/CNARules#section_4-1_Vulnerability_Determination
- https://www.youtube.com/watch?v=2VB4Zd5C8N8&t=39s
- https://nvd.nist.gov/vuln-metrics/cvss#:~:text=The%20Common%20Vulnerability%20Scoring%20System,Base%2C%20Temporal%2C%20and%20Environmental.
- https://alus.com.br/10-exploits-cves-que-preocupam-os-profissionais-da-ciberseguranca/