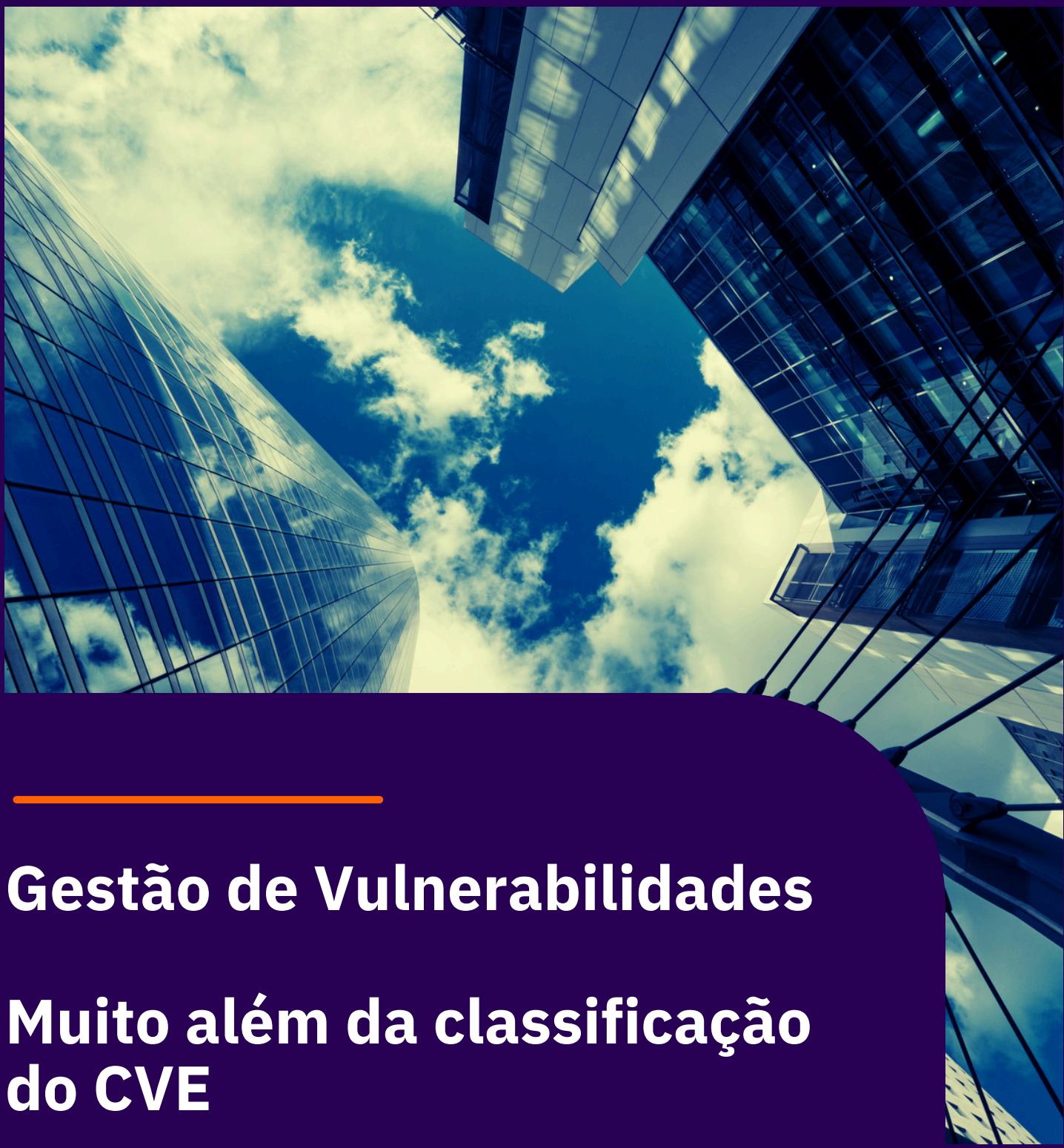
LUCAS ARANTES GUILHERME CARDOSO VULNERI.IO



# Gestão de Vulnerabilidades

# Muito além da classificação do CVE

Um guia prático para determinar a real criticidade e priorizar o tratamento das vulnerabilidades em sistemas de informação

# Conteúdo


01 Introdução

02 Principais Mantenedores

03 Devorando a Sopa de Letrinhas

04 Determinar a Real Criticidade da Vulnerabilidade

05 Priorizar a Correção através da árvore de decisão SSVC

06 Conclusão

# Autores

## LUCAS ARANTES

**Profissional com mais de 20 anos atuando em Infraestrutura de Tecnologia e Cyber Segurança. Ao longo de sua carreira, ele atuou como especialista e gestor em diversas empresas de grande porte, ajudando a desenvolver e implementar estratégias eficazes de defesa cibernética e gestão de vulnerabilidades.**

## GUILHERME CARDOSO

**Profissional com experiência na construção (de zero a um) e no crescimento de empresas de produtos, plataformas e consultoria de classe mundial, oferecendo experiências digitais ao cliente, plataformas digitais e aplicativos e sistemas corporativos. Sólida experiência em gestão e estratégia, engenharia de software, arquitetura de software e consultoria, com foco em disciplinas de Application Lifecycle Management (ALM) e DevOps.**

**A VULNERI É UMA PLATAFORMA DE CYBER SEGURANÇA QUE ATUA DE MANEIRA PROATIVA E CONTÍNUA, ANALISANDO AMBIENTES DE TECNOLOGIA. ENTREGAMOS FERRAMENTAS PARA QUE OS TIMES ATUEM DE MANEIRA MAIS EFETIVA NA MITIGAÇÃO DE RISCOS E VULNERABILIDADES.**

# Introdução

Em um mundo cada vez mais digital, a segurança da informação se tornou uma prioridade crítica para organizações de todos os tamanhos. Vulnerabilidades em sistemas e aplicações podem ser exploradas por hackers, resultando em perda de dados, interrupções nos negócios e danos à reputação. Para mitigar esses riscos, é essencial adotar processos robustos de gestão de vulnerabilidades.

A gestão de vulnerabilidades é um processo contínuo que envolve a identificação, avaliação, tratamento e monitoramento de fraquezas em sistemas de informação. Este processo é fundamental para garantir a segurança e a resiliência das infraestruturas digitais. Importantes organizações e agências governamentais fornecem diretrizes e melhores práticas para a implementação eficaz da gestão de vulnerabilidades.

**Vulneri Tecnologia e Seguranca Digital LTDA**
**Av. Paulista, 1106, Bela Vista, São Paulo - SP**
**https://vulneri.io**
**contato@vulneri.io**

**+55 11 91221 3983**

**Entre em contato**

# Principais Mantenedores

**Antes de mergulharmos nas siglas e seus significados, é importante conhecer os principais mantenedores desses sistemas e padrões**

### MITRE CORPORATION

Uma organização sem fins lucrativos que gerencia diversas iniciativas críticas para a segurança cibernética, incluindo o CVE (Common Vulnerabilities and Exposures), o CWE (Common Weakness Enumeration) e o CAPEC (Common Attack Pattern Enumeration and Classification).

### FIRST

Forum of Incident Response and Security Teams

Organização global dedicada a melhorar a resposta a incidentes de segurança cibernética. Mantém o CVSS (Common Vulnerability Scoring System) e o EPSS (Exploit Prediction Scoring System).

### CISA

Cybersecurity and Infrastructure Security Agency

Agência do governo dos EUA responsável pela segurança cibernética e infraestrutura crítica. Mantém a base de dados de Vulnerabilidades Conhecidas e Exploradas (KEV).

### NIST

National Institute of Standards and Technology

Agência governamental dos EUA que desenvolve normas e diretrizes para melhorar a segurança cibernética em organizações. Mantém o NVD (National Vulnerability Database).

### CERT/CC

Computer Emergency Response Team Coordination Center

Unidade da Carnegie Mellon University que desenvolve metodologias como o SSVC (Stakeholder-Specific Vulnerability Categorization) para priorização de vulnerabilidades.

# Devorando a Sopa de Letrinhas

**Ao nos aprofundarmos nos processos de gestão de vulnerabilidades, frequentemente nos deparamos com um mar de siglas e acrônimos, popularmente conhecido como a famosa "sopa de letrinhas". Embora possa parecer confuso à primeira vista, cada uma dessas letrinhas desempenha um papel crucial na proteção dos nossos sistemas e dados. Vamos devorar essa sopa de letrinhas e entender por que cada ingrediente é essencial para a gestão de vulnerabilidades.**

## CVE

Common Vulnerabilities and Exposures

O CVE é um identificador único para vulnerabilidades conhecidas em software ou firmware, facilitando o compartilhamento de informações entre ferramentas de segurança. Mantido pela MITRE Corporation, com suporte da Agência de Segurança Cibernética e Infraestrutura (CISA) dos EUA

## CVSS

Common Vulnerability Scoring System - O CVSS é um sistema de pontuação que mede a gravidade das vulnerabilidades em uma escala de 0 a 10, ajudando a priorizar as respostas com base no risco. Desenvolvido e mantido pelo Forum of Incident Response and Security Teams (FIRST).

## EPSS

Exploit Prediction Scoring System

O EPSS estima a probabilidade de uma vulnerabilidade ser explorada no futuro, fornecendo uma pontuação que ajuda a priorizar vulnerabilidades com base na ameaça real. Mantido pelo Forum of Incident Response and Security Teams (FIRST).

## KEV

Known Exploited Vulnerabilities

O KEV é um catálogo de vulnerabilidades conhecidas por serem exploradas ativamente, mantido e gerido pela Cybersecurity and Infrastructure Security Agency (CISA) dos EUA

# Devorando a Sopa de Letrinhas

## NVD

National Vulnerability Database

O NVD é um repositório que inclui detalhes sobre CVEs, suas pontuações CVSS e outras informações de mitigação, mantido pelo National Institute of Standards and Technology (NIST) dos EUA.

## CWE

Common Weakness Enumeration

O CWE é um catálogo de fraquezas de software conhecidas que podem levar a vulnerabilidades, ajudando a entender e mitigar as causas raiz de problemas de segurança. Mantido pela MITRE Corporation.

## CWSS

Common Weakness Scoring System

O CWSS é um sistema de pontuação para classificar fraquezas de software, proporcionando uma visão mais profunda sobre a criticidade das fraquezas subjacentes. Desenvolvido e mantido pela MITRE Corporation.

## SSVC

Stakeholder-Specific Vulnerability Categorization

O SSVC é uma metodologia que auxilia na priorização de vulnerabilidades com base nas necessidades e perspectivas específicas dos diferentes stakeholders. Ele usa uma abordagem baseada em decisões, considerando fatores como a urgência e a importância das ações de mitigação. Desenvolvido pelo CERT/CC (Computer Emergency Response Team Coordination Center) da Carnegie Mellon University.

## CAPEC

Common Attack Pattern Enumeration and Classification

CAPEC é um catálogo de padrões de ataque conhecidos, oferecendo uma base de conhecimento estruturada sobre as táticas, técnicas e procedimentos (TTPs) que os atacantes utilizam. Este catálogo é útil para entender as metodologias de ataque e desenvolver estratégias de defesa. Mantido pela MITRE Corporation.

# Determinar a Real Criticidade da Vulnerabilidade

## PASSO 1: IDENTIFIQUE A VULNERABILIDADE COM CVE

**CVE (Common Vulnerabilities and Exposures)** é como um número de identidade para vulnerabilidades conhecidas. Cada CVE tem um código único, como CVE-2024-12345, que descreve uma vulnerabilidade específica.

*Exemplo:* Imagine que você encontra o CVE-2024-12345. Este código indica uma vulnerabilidade específica em um software.

## PASSO 2: AVALIE A CRITICIDADE COM CVSS

**CVSS (Common Vulnerability Scoring System)** fornece uma pontuação que vai de 0 a 10 para indicar a gravidade da vulnerabilidade. Pontuações mais altas significam problemas mais sérios.

*Exemplo:* CVE-2024-12345 tem uma pontuação CVSS de 9.0, indicando que é uma vulnerabilidade crítica. Já o CVE-2024-67890 tem uma pontuação CVSS de 7.5, o que indica uma gravidade alta, mas não crítica.

## PASSO 3: ESTIME A PROBABILIDADE DE EXPLORAÇÃO COM EPSS

**EPSS (Exploit Prediction Scoring System)** indica a probabilidade de que a vulnerabilidade seja explorada. Uma pontuação EPSS alta sugere que é mais provável que hackers explorem essa vulnerabilidade.

*Exemplo:* CVE-2024-12345 tem uma pontuação EPSS de 0.1, indicando baixa probabilidade de exploração. Em contraste, CVE-2024-67890 tem uma pontuação EPSS de 0.8, sugerindo alta probabilidade de ser explorada.

# Determinar a Real Criticidade da Vulnerabilidade

## PASSO 4: VERIFIQUE SE A VULNERABILIDADE É ATIVAMENTE EXPLORADA COM KEV

**KEV (Known Exploited Vulnerabilities)** é uma lista de vulnerabilidades que estão sendo ativamente exploradas por hackers. Se uma vulnerabilidade estiver na lista KEV, é uma prioridade alta para correção.

*Exemplo:* CVE-2024-67890 está listado no KEV, enquanto CVE-2024-12345 não está. Isso significa que CVE-2024-67890 está sendo explorado ativamente e requer atenção imediata.

## PASSO 5: OBTENHA INFORMAÇÕES DETALHADAS NO NVD

**NVD (National Vulnerability Database)** oferece detalhes adicionais sobre a vulnerabilidade, incluindo descrições detalhadas e recomendações de mitigação.

*Exemplo:* Consultando o NVD, você descobre que CVE-2024-67890 afeta um componente crítico do sistema e que há um patch disponível para corrigir o problema.

## PASSO 6: COMPREENDA A FRAQUEZA SUBJACENTE COM CWE

**CWE (Common Weakness Enumeration)** ajuda a entender a causa raiz da vulnerabilidade, categorizando-a em tipos de fraquezas de software.

*Exemplo:* CVE-2024-67890 está associado a CWE-79, que é uma fraqueza comum conhecida como Cross-Site Scripting (XSS). Saber disso ajuda a entender como a vulnerabilidade funciona e como preveni-la no futuro.

# Determinar a Real Criticidade da Vulnerabilidade

## PASSO 7: AVALIE A SEVERIDADE DA FRAQUEZA COM CWSS

**CWSS (Common Weakness Scoring System)** fornece uma pontuação que avalia a severidade das fraquezas subjacentes.

*Exemplo:* CWE-79 tem uma pontuação CWSS alta, indicando que fraquezas desse tipo são particularmente perigosas e devem ser tratadas com prioridade

## PASSO 8: ENTENDA OS PADRÕES DE ATAQUE COM CAPEC

**CAPEC (Common Attack Pattern Enumeration and Classification)** ajuda a entender as táticas e técnicas que os atacantes usam para explorar vulnerabilidades, permitindo que as organizações desenvolvam defesas mais eficazes.

Exemplo: CVE-2024-67890 está associado a um padrão de ataque CAPEC específico, como CAPEC-133: Cross-Site Scripting, o que fornece insights adicionais sobre como o ataque pode ocorrer e como se defender.

## PASSO 9: PRIORIZE AÇÕES DE MITIGAÇÃO COM SSVC

**SSVC (Stakeholder-Specific Vulnerability Categorization)** ajuda a priorizar ações de mitigação baseadas nas necessidades específicas dos stakeholders. Ele considera fatores como urgência e impacto potencial.

*Exemplo:* CVE-2024-67890 pode ser priorizado como urgente para correção porque afeta diretamente um componente crítico usado por uma grande parte dos usuários, conforme determinado pela metodologia SSVC.

# Correlacionando os Resultados

Identifique a vulnerabilidade com **CVE**

Avalie a gravidade com **CVSS**

Verifique a probabilidade de exploração com **EPSS**

Veja se está sendo explorada ativamente com **KEV**

Consulte detalhes adicionais e mitigações no **NVD**

Entenda a fraqueza subjacente com **CWE**

Avalie a severidade da fraqueza com **CWSS**

Entenda os padrões de ataque com **CAPEC**

Priorize as ações de mitigação com **SSVC**

# Exemplos de Interpretação

### Vulnerabilidade 1: CVE-2024-12345

CVSS: 9.0 (Crítico)
EPSS: 0.1 (Baixa probabilidade de exploração)
KEV: Não listado
NVD: Detalhes disponíveis, mitigação sugerida
CWE: Não relevante
CWSS: Não relevante
CAPEC: Não relevante
SSVC: Baixa prioridade de mitigação

### Vulnerabilidade 2: CVE-2024-67890

CVSS: 7.5 (Alto)
EPSS: 0.8 (Alta probabilidade de exploração)
KEV: Listado (Exploração ativa)
NVD: Detalhes disponíveis, patch disponível
CWE: CWE-79 (Cross-Site Scripting)
CWSS: Alta severidade
CAPEC: CAPEC-133 (Cross-Site Scripting)
SSVC: Alta prioridade de mitigação

**Mesmo que o CVE-2024-12345 tenha uma pontuação CVSS mais alta, o CVE-2024-67890 é mais crítico devido à alta probabilidade de exploração, exploração ativa e impacto significativo. Portanto, o CVE-2024-67890 deve ser tratado com maior prioridade. Mas qual prioridade?**

# Priorizando a correção da Vulnerabilidade através da árvore de decisão da SSVC

**A árvore de decisão SSVC (Stakeholder-Specific Vulnerability Categorization) é uma metodologia desenvolvida pela Carnegie Mellon University para aprimorar a priorização de vulnerabilidades com base em variáveis específicas ao contexto do ambiente e das necessidades dos stakeholders. Diferente de métodos tradicionais que se baseiam exclusivamente em pontuações de gravidade, como o CVSS, o SSVC incorpora um conjunto mais amplo de fatores, permitindo decisões mais contextualizadas e eficazes.**

## VARIÁVEIS CONSIDERADAS NA ÁRVORE DE DECISÃO SSVC

- **Status de Exploração da Vulnerabilidade:**
  - Determina se a vulnerabilidade está sendo ativamente explorada (informações frequentemente derivadas de fontes como a KEV).

- **Exposição Externa do Sistema:**
  - Avalia se o sistema afetado está exposto à internet, o que pode aumentar significativamente o risco de exploração.

- **Valor da Vulnerabilidade do Ponto de Vista do Atacante:**
  - Considera o quão atrativa a vulnerabilidade é para os atacantes, especialmente se permite execuções remotas de código (RCEs) ou outras ações críticas.

- **Impacto no Negócio:**
  - Mede o impacto potencial que a exploração da vulnerabilidade teria nas operações do negócio, diferenciando entre sistemas críticos e não críticos.

# Priorizando a correção da Vulnerabilidade através da árvore de decisão da SSVC

## CLASSIFICAÇÃO DAS RESPOSTAS

**A árvore de decisão do SSVC categoriza as vulnerabilidades em quatro níveis de prioridade de resposta:**

**Imediato: Ação imediata é necessária**

**Fora do Ciclo: Requer resposta urgente, mas não imediata**

**Programado: Pode ser tratado durante a próxima manutenção programada.**

**Adiado: Pode ser tratado posteriormente quando conveniente.**

Seguindo a árvore de decisão do SSVC é possível determinar a prioridade das ações de mitigação com base em um entendimento mais profundo do risco real e do impacto específico no seu ambiente. Isso resulta em uma abordagem mais eficiente e eficaz para a gestão de vulnerabilidades.

# Exemplo Detalhado Usando a Árvore de Decisão do SSVC

Vamos usar a árvore de decisão do SSVC para avaliar dois exemplos de vulnerabilidades: CVE-2024-12345 e CVE-2024-67890.

## Variáveis Consideradas no SSVC

### Status de Exploração da Vulnerabilidade:

**Está sendo explorada ativamente?**

### Exposição Externa do Sistema:

**O sistema está exposto à internet?**

### Valor da Vulnerabilidade do Ponto de Vista do Atacante:

**A vulnerabilidade é atrativa para atacantes, como no caso de execuções remotas de código (RCEs)?**

### Impacto no Negócio:

**Qual o impacto da exploração da vulnerabilidade nas operações do negócio?**

# Exemplo Detalhado Usando a Árvore de Decisão do SSVC

## EXEMPLO 1 | CVE-2024-12345

CVSS: 9.0 (Crítico)
EPSS: 0.1 (Baixa probabilidade de exploração)
KEV: Não listado

**Análise com SSVC**

Status de Exploração da Vulnerabilidade:
Não está sendo explorada ativamente (não listado no KEV)

Exposição Externa do Sistema:
Sistema Interno: Não exposto à internet

Valor da Vulnerabilidade do Ponto de Vista do Atacante:
Não atrativa - EPSS baixo (0.1), indicando baixa probabilidade de exploração

Impacto no Negócio:
Impacto Médio - A exploração pode causar interrupções, mas não é em um sistema crítico.

**Decisão SSVC**

Classificação: Programado

Ação: Tratar durante a próxima janela de manutenção programada.

# Exemplo Detalhado Usando a Árvore de Decisão do SSVC

## EXEMPLO 2 | CVE-2024-67890

CVSS: 7.5 (Alto)
EPSS: 0.8 (Alta probabilidade de exploração)
KEV: Listado (Exploração Ativa)

**Análise com SSVC**

Status de Exploração da Vulnerabilidade:
Está sendo explorada ativamente (listado no KEV)

Exposição Externa do Sistema:
Sistema Externo: Exposto à internet

Valor da Vulnerabilidade do Ponto de Vista do Atacante:
Altamente atrativa - EPSS alto (0.8), indicando alta probabilidade de exploração

Impacto no Negócio:
Impacto Alto - A exploração pode afetar um sistema crítico, potencialmente interrompendo operações de negócios

**Decisão SSVC**

Classificação: Imediato

Ação: Tratar imediatamente devido à alta probabilidade de exploração e impacto crítico no negócio.

# Conclusão

Para determinar a criticidade real de uma vulnerabilidade, é importante olhar além da pontuação CVSS. Considere a probabilidade de exploração (EPSS), verifique se está sendo ativamente explorada (KEV), consulte detalhes adicionais (NVD), entenda a fraqueza subjacente (CWE), avalie a severidade da fraqueza (CWSS), entenda os padrões de ataque (CAPEC) e priorize as ações de mitigação (SSVC).

O SSVC adiciona uma camada crítica de sofisticação à gestão de vulnerabilidades, permitindo uma priorização baseada em variáveis contextuais específicas, como o status de exploração da vulnerabilidade, a exposição do sistema, o valor da vulnerabilidade do ponto de vista do atacante e o impacto no negócio. Esta abordagem oferece uma priorização mais precisa e eficaz, que vai além das limitações dos métodos tradicionais baseados em pontuações de gravidade.

Usando todas essas informações, você pode tomar decisões mais informadas e priorizar as vulnerabilidades de forma eficaz.

A VULNERI É UMA PLATAFORMA DE CYBER SEGURANÇA QUE ATUA DE MANEIRA PROATIVA E CONTÍNUA, ANALISANDO AMBIENTES DE TECNOLOGIA. ENTREGAMOS FERRAMENTAS PARA QUE OS TIMES ATUEM DE MANEIRA MAIS EFETIVA NA MITIGAÇÃO DE RISCOS E VULNERABILIDADES.

+55 11 91221 3983

Entre em contato