Centro de
Investigación en
Computación

NIST

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Ejemplos de Estándares
3. CMMC
4. NVD
5. Resumen

Introducción

Definiciones

Introducción

Definiciones

- It is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.
- A partir de 1988 cambio su nombre (antes *National Bureau of Standards*, NBS) y su mission se centro en la creación de estándares en diversas áreas.

Menú de página web

Advanced communications	Environment	Metrology
Artificial intelligence	Fire	Nanotechnology
Bioscience	Forensic science	Neutron research
Buildings and construction	Health	Performance excellence
Chemistry	Information technology	Physics
Cybersecurity	Infrastructure	Public safety
Electronics	Manufacturing	Quantum information science
Energy	Materials	Resilience
	Mathematics and statistics	Standards
		Transportation

- Referencias
  - https://www.nist.gov/

En México es la NOM (Norma Oficial Mexicana)

- https://www.gob.mx/se/acciones-y-programas/standards
- https://catalogomexicanodenormas.economia.gob.mx/

Introducción

Definiciones

- Tiene muchas actividades y material y sobre todo en el área de la educación.
- El material (*Resources*) se encuentra bajo el rubro:
  - *Computer Security Resource Center* (CSRC)
  - https://csrc.nist.gov/
- La mayoría de sus documentos siguen el formato:

  NIST Special Publication Número-Número

  Por ejemplo:

  NIST SP 800-152

  A Profile for U.S. Federal *Cryptographic Key Management Systems*
- Como es mucho el material, a continuación, solo presentaremos algunos de los trabajos más importantes.

Introducción

Definiciones

Frameworks / Marco de Trabajo

Es un conjunto estructurado de conceptos, buenas prácticas, herramientas y reglas que sirven como base para desarrollar soluciones en un área específica.

CYBERSECURITY

Frameworks −

1. Cybersecurity Framework
2. Privacy Framework
3. Risk Management Framework
4. NICE Workforce Framework for Cybersecurity

National Cybersecurity Center of Excellence (NCCoE)

NICE

Cybersecurity, Privacy, and AI

Small Business Cybersecurity Corner

Stakeholder Engagement

Computer Security Resource Center (CSRC)

NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

Some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems. Our cybersecurity activities also are driven by the needs of U.S. industry and the broader public. We engage vigorously with stakeholders to set priorities and ensure that our resources address the key issues that they face.

NIST also advances understanding and improves the management of privacy risks, some of which relate directly to cybersecurity.

Priority areas to which NIST contributes – and plans to focus more on – include cryptography, education and workforce,

Introducción

Definiciones

Glosario

- Tiene: 9,907 records.
- Se puede consultar:
  - En línea:

    https://csrc.nist.gov/glossary
  - Descargar en formato Json.
- Todas las definiciones son tomadas de sus documentos y hacen referencia a ellas en ese contexto.
- Son definiciones de referencia muy buenas.

Ejemplos de Estándares

En ciberseguridad

Lista

Ejemplos

Lista

De todos los trabajos del NIST los mas importantes son:

- Frameworks: los 4 estándares.
- National Vulnerability Database (NVD)
  - Common Vulnerability Scoring System (CVSS).
- Ejemplos
  - NIST SP 800-12 An Introduction to Information Security
  - NIST SP 800-30 **Risk** Management Guide for Information Technology Systems
  - NIST SP 800-53 Security and Privacy **Controls** for Information Systems and Organizations
  - NIST SP 800-61 Computer Security **Incident** Handling Guide
  - NIST SP 800-152 A Profile for U.S. Federal **Cryptographic** Key Management Systems
  - NIST SP 800-171 Security Requirements for Protecting Controlled Unclassified **Information**
  - NIST 1800 Series: Cybersecurity Practice Guides, https://csrc.nist.gov/publications/sp1800
- Descargas
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
  - https://doi.org/10.6028/NIST.SP.800-53r5

Ejemplos

Lista

Federal Information Processing Standards (FIPS)

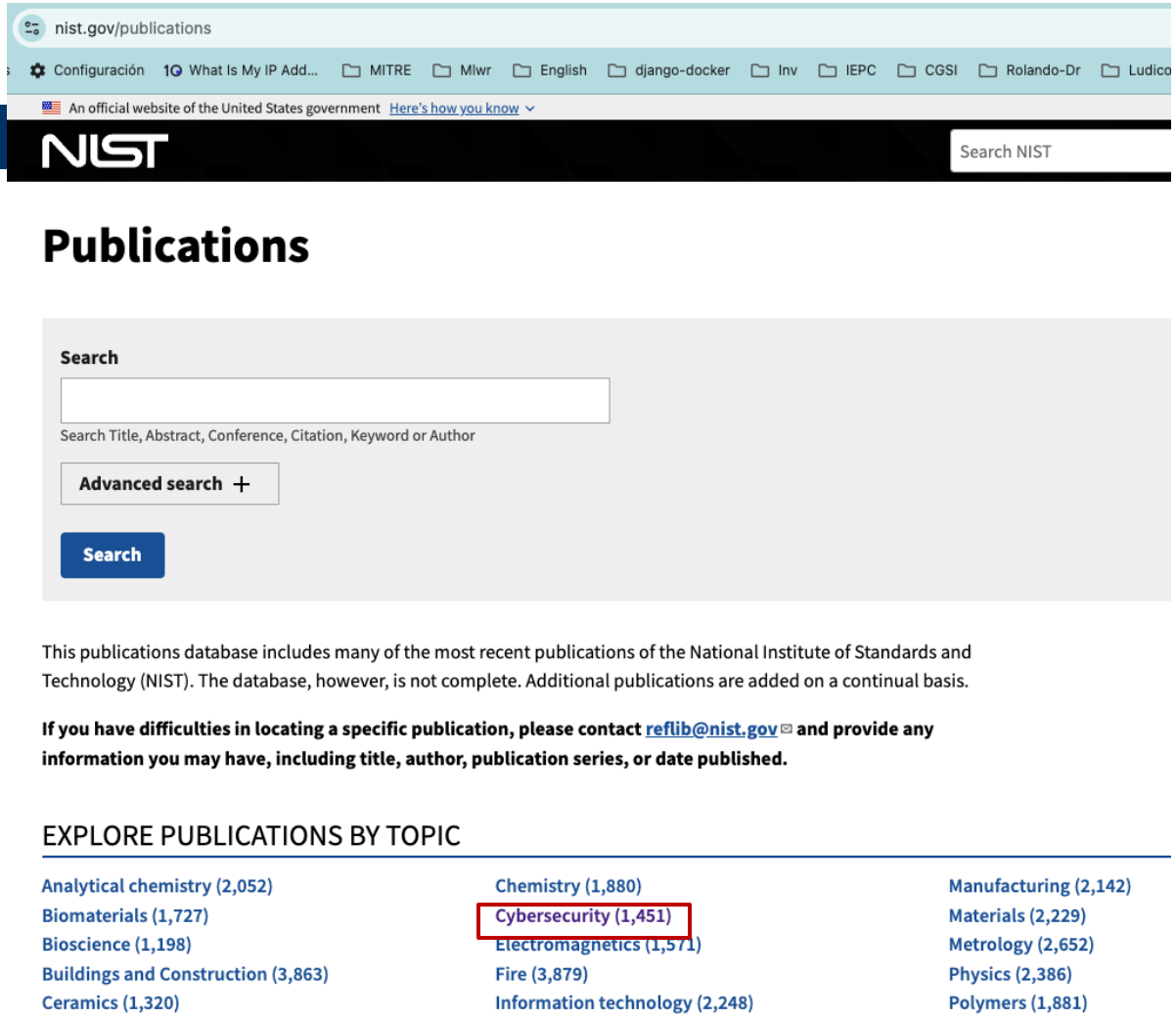
- FIPS are standards for federal computer systems that are developed by the NIST and approved by the Secretary of Commerce.
- These standards are developed when there are no acceptable industry standards or solutions for a particular government requirement. Although FIPS are developed for use by the Federal Government, many in the private sector voluntarily use these standards.
- FIPS Publications (FIPS PUBS)
- Ejemplos
  - FIPS 140-2 Security Requirements for Cryptographic Modules. Superseded By: FIPS 140-3
  - FIPS186-4 Digital Signature Standard (DSS)
  - FIPS 197 Advanced Encryption Standard (AES)

NIST Interagency or Internal Reports (NISTIR)

- NIST IR 7298 Glossary of Key Information Security Terms
- NISTIR 8165 Impact of Code Complexity On Software Analysis

Ejemplos

Lista



Ejemplos

Lista

NIST 1800 Series

Series	Number	Title	Status	Release Date
SP	1800-40	Automation of the NIST Cryptographic Module Validation Program	Draft	6/07/2023
SP	1800-39	Implementing Data Classification Practices	Draft	4/25/2023
SP	1800-38	Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography	Draft	12/19/2023
SP	1800-37	Addressing Visibility Challenges with TLS 1.3 within the Enterprise	Draft	1/30/2024
SP	1800-36	Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security	Draft	5/31/2024
SP	1800-35	Implementing a Zero Trust Architecture	Draft	12/04/2024
SP	1800-34	Validating the Integrity of Computing Devices	Final	12/09/2022
SP	1800-33	5G Cybersecurity	Draft	4/25/2022
SP	1800-32	Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity	Final	2/02/2022
SP	1800-31	Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways	Final	4/06/2022
SP	1800-30	Securing Telehealth Remote Patient Monitoring Ecosystem	Final	2/22/2022
SP	1800-29	Data Confidentiality: Detect, Respond to, and Recover from Data Breaches	Final	2/23/2024
SP	1800-28	Data Confidentiality: Identifying and Protecting Assets Against Data Breaches	Final	2/23/2024
SP	1800-27	Securing Property Management Systems	Final	3/30/2021
SP	1800-26	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events	Final	12/08/2020
SP	1800-25	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events	Final	12/08/2020
SP	1800-24	Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector	Final	12/21/2020
SP	1800-23	Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry	Final	5/20/2020
SP	1800-22	Mobile Device Security: Bring Your Own Device (BYOD)	Final	9/28/2023
SP	1800-21	Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)	Final	9/15/2020
SP	1800-19	Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments	Final	4/20/2022
SP	1800-17	Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers	Final	7/30/2019
SP	1800-16	Securing Web Transactions: TLS Server Certificate Management	Final	6/16/2020
SP	1800-15	Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)	Final	5/26/2021

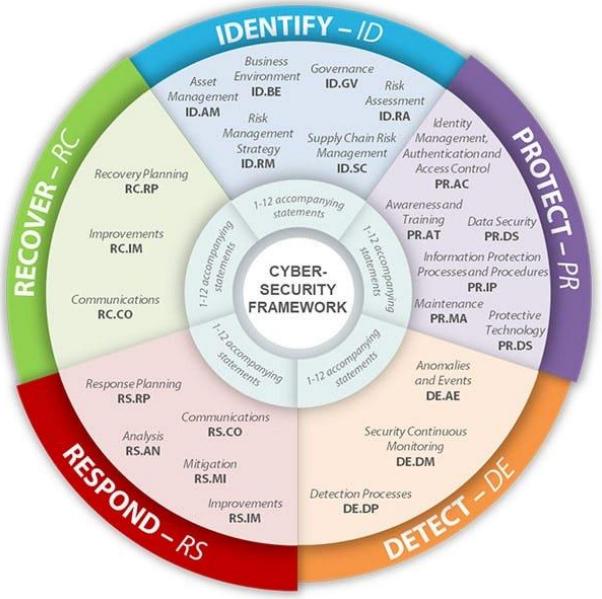
CSF

The NIST **C**yber**S**ecurity **F**ramework 2.0

Resource

CSF

Intro



Características:

- Sirve para gestionar y reducir riesgos de seguridad.
- Esta formado por 3 components: CSF Core, CSF Organizational Profiles, y CSF Tiers (niveles).
- El CSF Core tiene 5 funciones:
  1. Indetify. Activos, riesgos, y regulaciones.
  2. Protect. Implementar controles de seguridad.
  3. Detect. Amenazas y anomalias.
  4. Respod. Gestionar incidentes
  5. Recover. Restaurar operaciones en caso de ataque.

Fuentes

- NIST CSWP 29.
- https://www.nist.gov/cyberframework

CSF

Intro

COBIT
Control **OB**jectives for **I**nformation and Related **T**echnologies
Objetivos de control para la información y tecnologías relacionadas

NIST CSF 2.0 vs COBIT

- Ambos son marcos de gobernanza diseñados para ayudar a las organizaciones a mejorar su ciberseguridad y gobernanza de TI, pero tienen diferentes propósitos:

- COBIT se centra en la gobernanza y la gestión de TI en general, y proporciona pautas para gestionar los riesgos, los recursos y el rendimiento relacionados con TI. COBIT es más integral en términos de gobernanza y proporciona un enfoque general para la gestión de TI.

- NIST CSF 2.0 se centra más en la gestión de riesgos de ciberseguridad y proporciona un marco detallado para crear y mejorar las capacidades de ciberseguridad dentro de una organización.

CMMC

Cybersecurity Maturity Model Certification

Resource

CMMC

Intro

Fue desarrollado por el NIST y es usado por la CISA:

- *Cybersecurity is a top priority for the Department of Defense (DoD).*
- El propósito del CMMC es verificar que los sistemas de información utilizados por los contratistas del Departamento de Defensa de EU para procesar, transmitir o almacenar datos confidenciales cumplan con los requisitos obligatorios de seguridad de la información.
- El objetivo es garantizar la protección adecuada de la información no clasificada controlada (CUI) y la información de contratos federales (FCI) que es almacenada y procesada por el socio o proveedor.

Fuentes

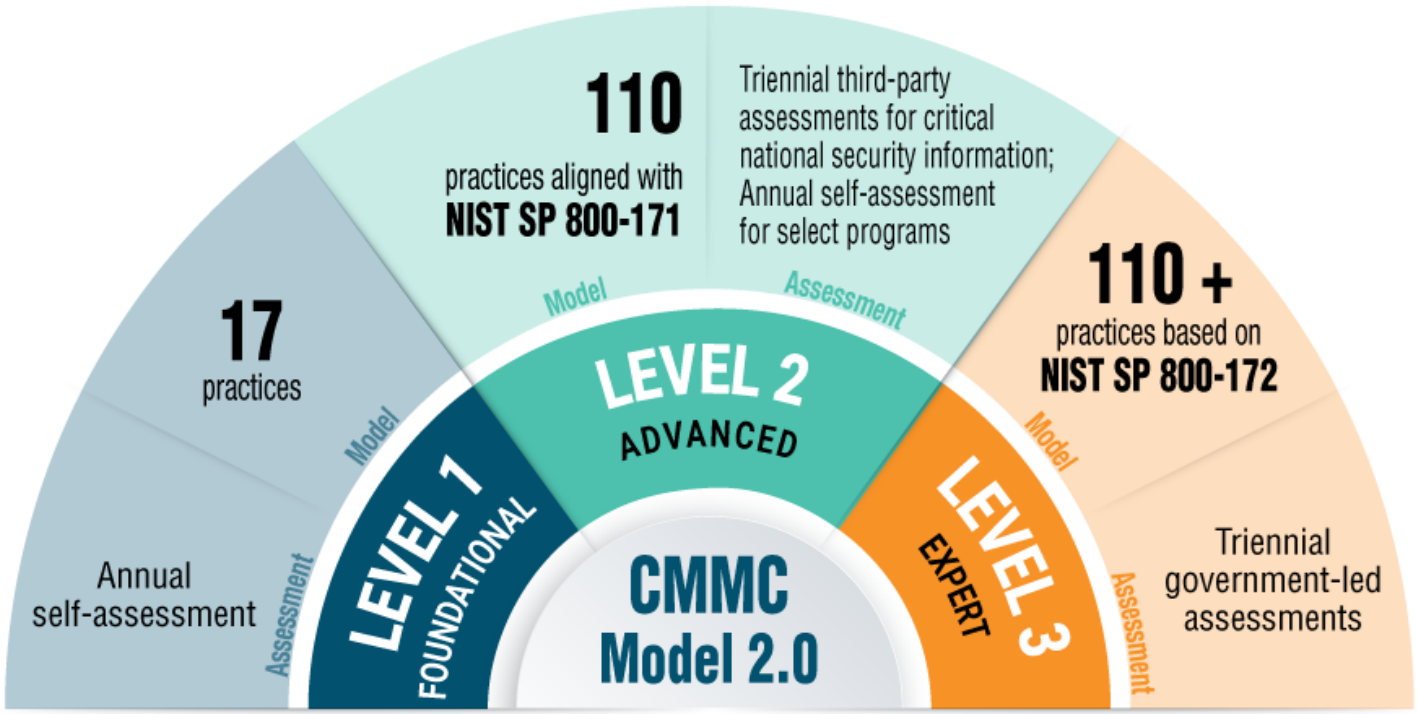
- https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program
- https://dodcio.defense.gov/CMMC/Model/

CMMC

Intro

CMMC Model 1.0			
Level	Model		Assessment
Level 5 Advanced (CUI, CRITICAL PROGRAMS)	171 practices	5 processes	Third-party
Level 4 Proactive (TRANSITION LEVEL)	156 practices	4 processes	None
Level 3 Good (CUI)	130 practices	3 processes	Third-party
Level 2 Intermediate (TRANSITION LEVEL)	72 practices	2 maturity processes	None
Level 1 Basic (FCI ONLY)	17 practices		Third-party

CMMC Model 2.0		
Level	Model	Assessment
Level 3 Expert	110+ practices based on NIST SP 800-171	Triannual government-led assessments
Level 2 Advanced	110 practices aligned with NIST SP 800-171	Triannual third-party assessments for critical national security information: Annual self-assessment for select programs
Level 1 Foundational	17 practices	Annual self-assessment



CMMC

Intro

Ejemplos detallado

- Se describen:
  - Control de Acceso
  - Concienciación y Capacitación
  - Auditoría y Responsabilidad
  - Gestión de Configuración
  - Identificación y Autenticación
  - Respuesta a Incidentes
  - Mantenimiento
  - Protección de Medios
  - Seguridad del Personal
  - Protección Física
  - Evaluación de Riesgos
  - Evaluación de Seguridad
  - Protección de Sistemas y Comunicaciones
  - Integridad del Sistema e Información
- URL
  - https://www.kiteworks.com/es/guia-mapeo-de-cumplimiento-cmmc-2-0-para-comunicaciones-de-contenido-confidencial/

National Vulnerability Database

NVD

Resource

NVD

Definición

The NVD is the U.S. government **repository** of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables:

- Automation of vulnerability management.
- Security measurement, and
- Compliance.

Se propone el CVSS que veremos más adelante

The NVD includes:

- Databases of security checklist references.
- Security-related software flaws.
- Product names, and
- Impact metrics.

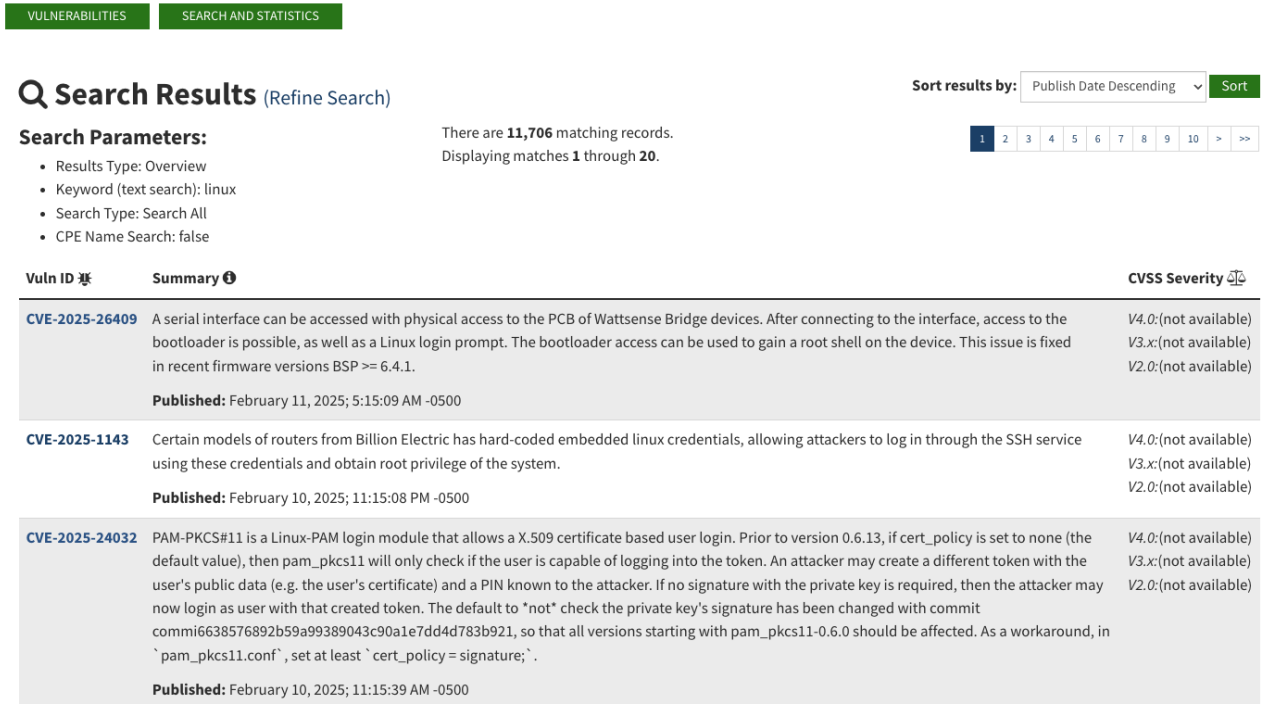
NVD

Definición

Búsqueda

- https://nvd.nist.gov/vuln/search

Ejemplo con “linux”



VULNERABILITIES | SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending | Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): linux
- Search Type: Search All
- CPE Name Search: false

There are **11,706** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2025-26409	A serial interface can be accessed with physical access to the PCB of Wattsense Bridge devices. After connecting to the interface, access to the bootloader is possible, as well as a Linux login prompt. The bootloader access can be used to gain a root shell on the device. This issue is fixed in recent firmware versions BSP >= 6.4.1. **Published:** February 11, 2025; 5:15:09 AM -0500	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)
CVE-2025-1143	Certain models of routers from Billion Electric has hard-coded embedded linux credentials, allowing attackers to log in through the SSH service using these credentials and obtain root privilege of the system. **Published:** February 10, 2025; 11:15:08 PM -0500	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)
CVE-2025-24032	PAM-PKCS#11 is a Linux-PAM login module that allows a X.509 certificate based user login. Prior to version 0.6.13, if cert_policy is set to none (the default value), then pam_pkcs11 will only check if the user is capable of logging into the token. An attacker may create a different token with the user's public data (e.g. the user's certificate) and a PIN known to the attacker. If no signature with the private key is required, then the attacker may now login as user with that created token. The default to *not* check the private key's signature has been changed with commit commi6638576892b59a99389043c90a1e7dd4d783b921, so that all versions starting with pam_pkcs11-0.6.0 should be affected. As a workaround, in `pam_pkcs11.conf`, set at least `cert_policy = signature;`. **Published:** February 10, 2025; 11:15:39 AM -0500	*V4.0:*(not available) *V3.x:*(not available) *V2.0:*(not available)

NVD

CVE-2024-57949 Detail

Description

In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v3-its: Don't enable interrupts in its_irq_set_vcpu_affinity() The following call-chain leads to enabling interrupts in a nested interrupt disabled section: irq_set_vcpu_affinity() irq_get_desc_lock() raw_spin_lock_irqsave() <--- Disable interrupts its_irq_set_vcpu_affinity() guard(raw_spinlock_irq) <--- Enables interrupts when leaving the guard() irq_put_desc_unlock() <--- Warns because interrupts are enabled This was broken in commit b97e8a2f7130, which replaced the original raw_spin_[un]lock() pair with guard(raw_spinlock_irq). Fix the issue by using guard(raw_spinlock). [tglx: Massaged change log]

QUICK INFO

CVE Dictionary Entry: CVE-2024-57949
NVD Published Date: 02/09/2025
NVD Last Modified: 02/11/2025
Source: kernel.org

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 5.5 MEDIUM **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://git.kernel.org/stable/c/35cb2c6ce7da545f3b5cb1e6473ad7c3a6f08310	Patch
https://git.kernel.org/stable/c/6c84ff2e788fce0099ee3e71a3ed258b1ca1a223	Patch
https://git.kernel.org/stable/c/93955a7788121ab5a0f7f27e988b2ed1135a4866	Patch
https://git.kernel.org/stable/c/d7b0e89610dd45ac6cf0d6f99bfa9ccc787db344	Patch

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-667	Improper Locking	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	From (including)	Up to (excluding)
Show Matching CPE(s)	6.1.95	6.1.127

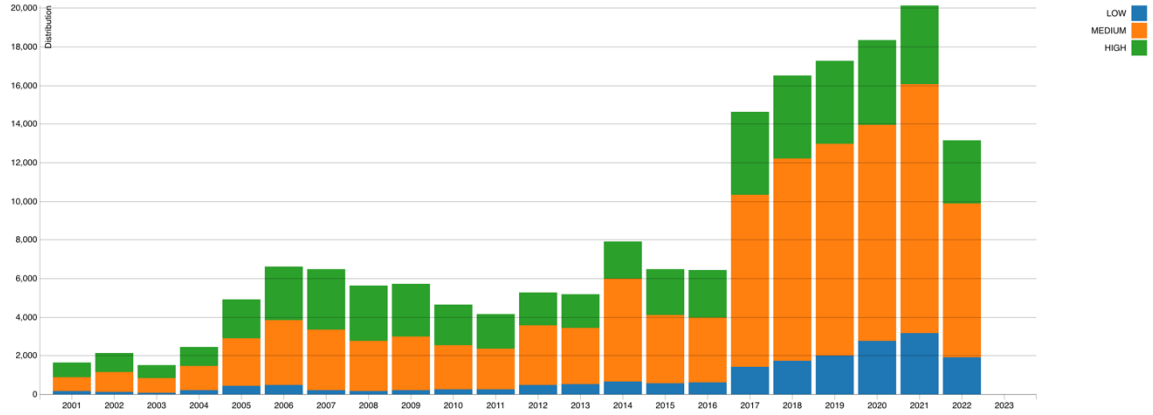
NVD

Definición

NVD visualizaciones

CVSS Severity Distribution Over Time

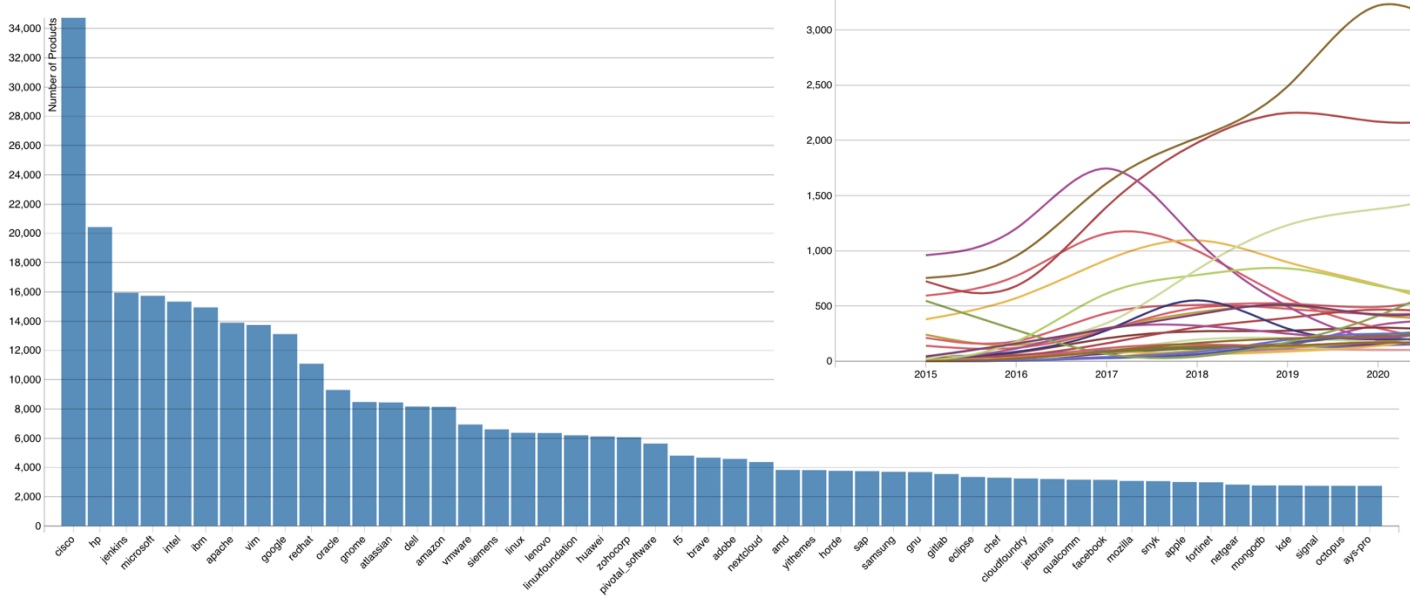
This visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score. For more information on how this data was constructed please see the NVD CVSS page .



CPE Products Distribution

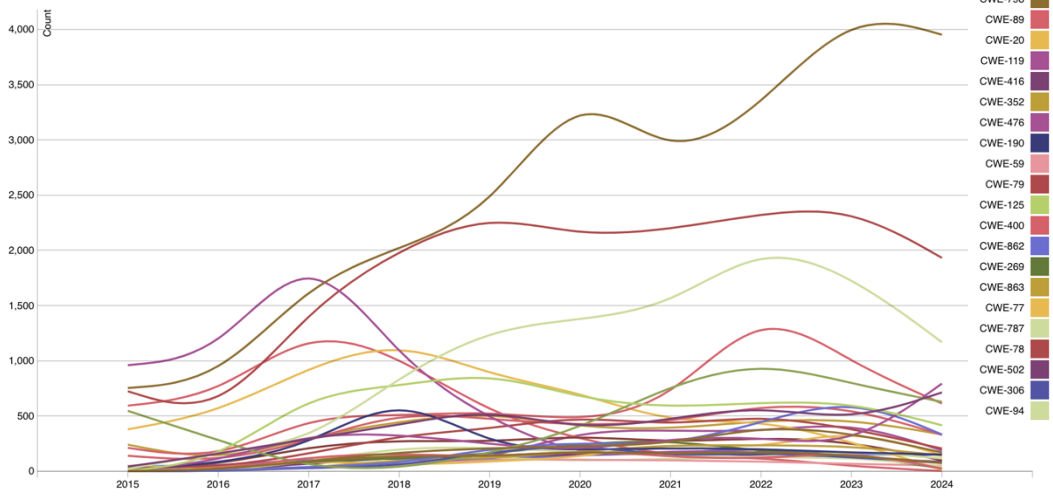
This visualization was generated using the vendor component of the CPE an
a distribution of the number of products by vendor available in the CPE dicti

Interactive: Hovering over a bar will show a tooltip containing the total number of products counted for
to a maximum of 20.



Vulnerability Type Change By Year

This visualization is a slightly different view that emphasizes how the assignment of CWEs has changed from year to year.



NVD

Definición

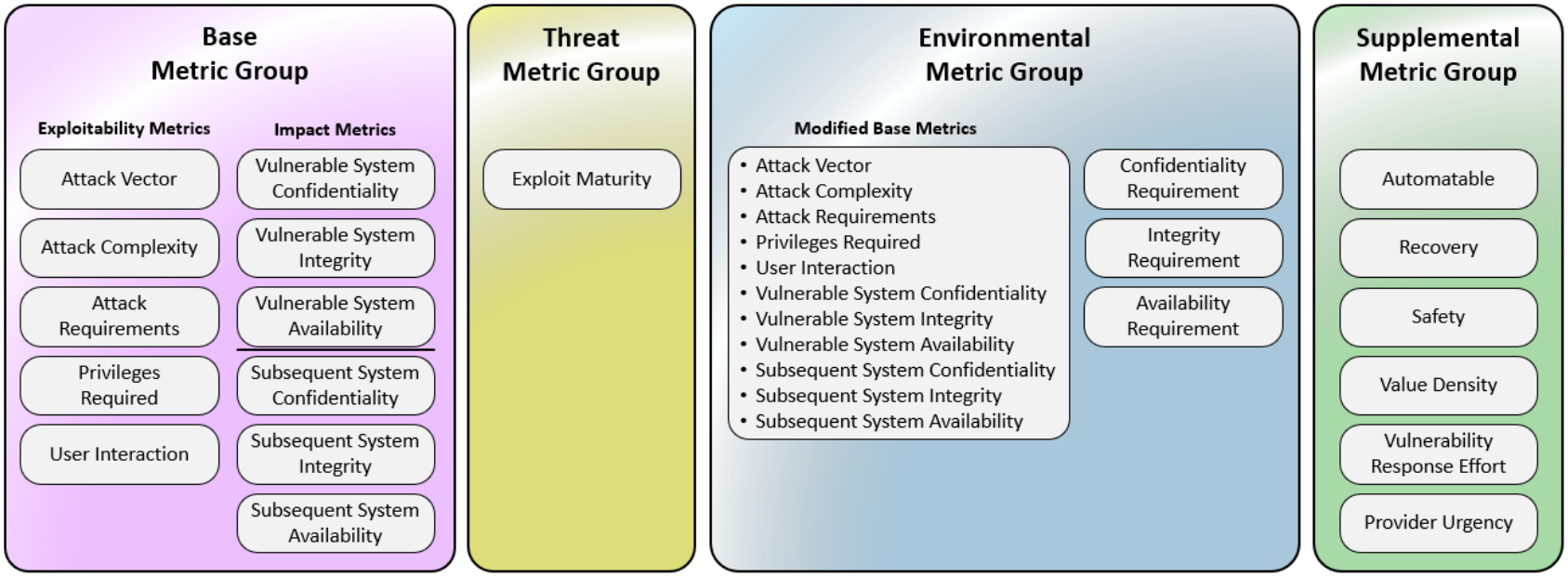
CVSS Common Vulnerability Scoring System

- It is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of four metric groups: Base, Threat, Environmental, and Supplemental.
  1. **Base**. Represents the intrinsic qualities of a vulnerability that are constant over time and across user environments.
  2. **Threat**. Reflects the characteristics of a vulnerability that change over time.
  3. **Environmental**. Represents the characteristics of a vulnerability that are unique to a user's environment.
  4. **Supplemental**. Ddo not modify the final score, and are used as additional insight into the characteristics of a vulnerability.
- Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics.
- To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations.
- It produces a score ranging from 0 to 10.

NVD

Definición

CVSS Nomenclature	CVSS Metrics Used
CVSS-B	Base metrics
CVSS-BE	Base and Environmental metrics
CVSS-BT	Base and Threat metrics
CVSS-BTE	Base, Threat, Environmental metrics



NVD

Definición

El FISRT tiene más material de ciberseguridad (disponible en su sitio) que por razones de tiempo solo se recomienda su lectura.
En particular la sección *Education -> Trainning*

CVSS

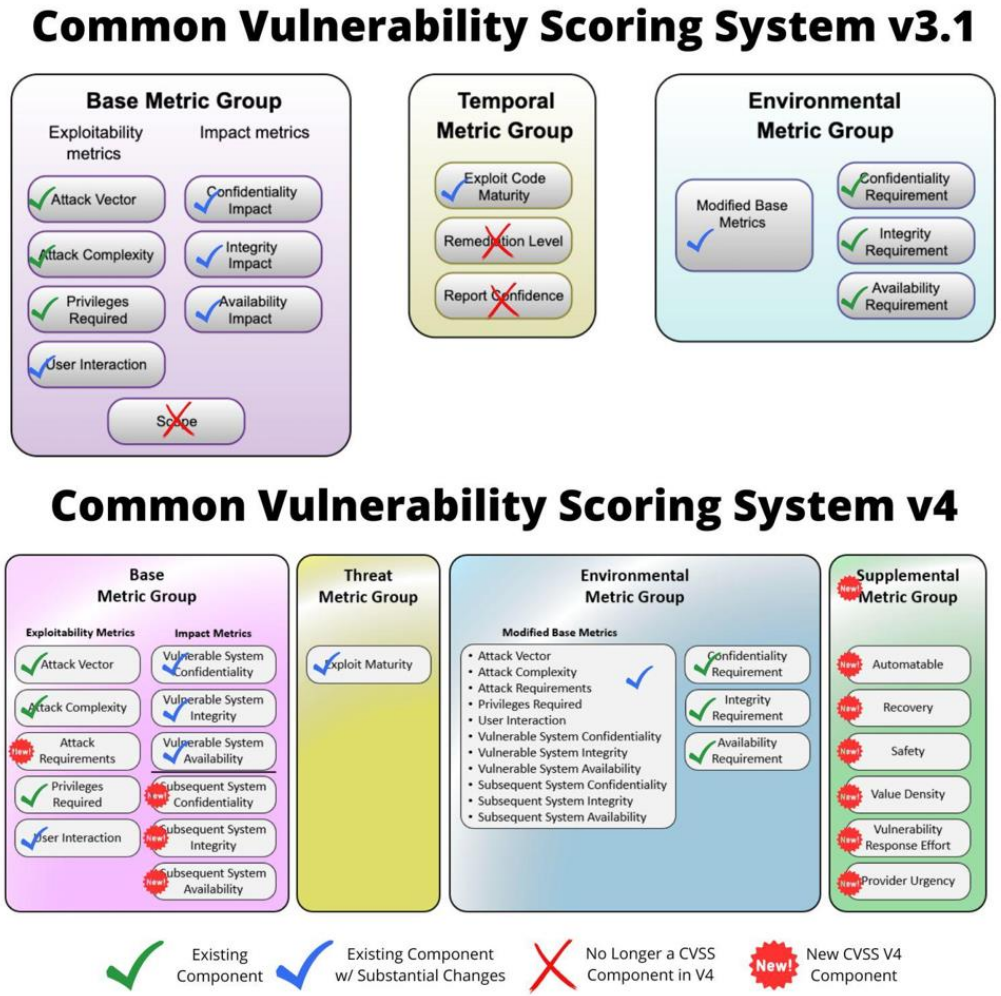
- Fue creado por el FIRST y adoptado por el NIST
  - **F**orum of **I**ncident **R**esponse and **S**ecurity **T**eams
- Hay 3 versiones disponibles: 2, 3 y 4.
- Referencias
  - https://www.first.org/cvss/user-guide
  - https://www.first.org/cvss/v4.0/specification-document
- CVSS v4.0 Calculator
  - https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator
  - https://www.first.org/cvss/calculator/4.0
- Los estándares no son muy didácticos asi que es mejor consultar otras fuentes:
  - https://www.picussecurity.com/resource/glossary/what-is-common-vulnerability-scoring-system-cvss

NVD

Definición

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

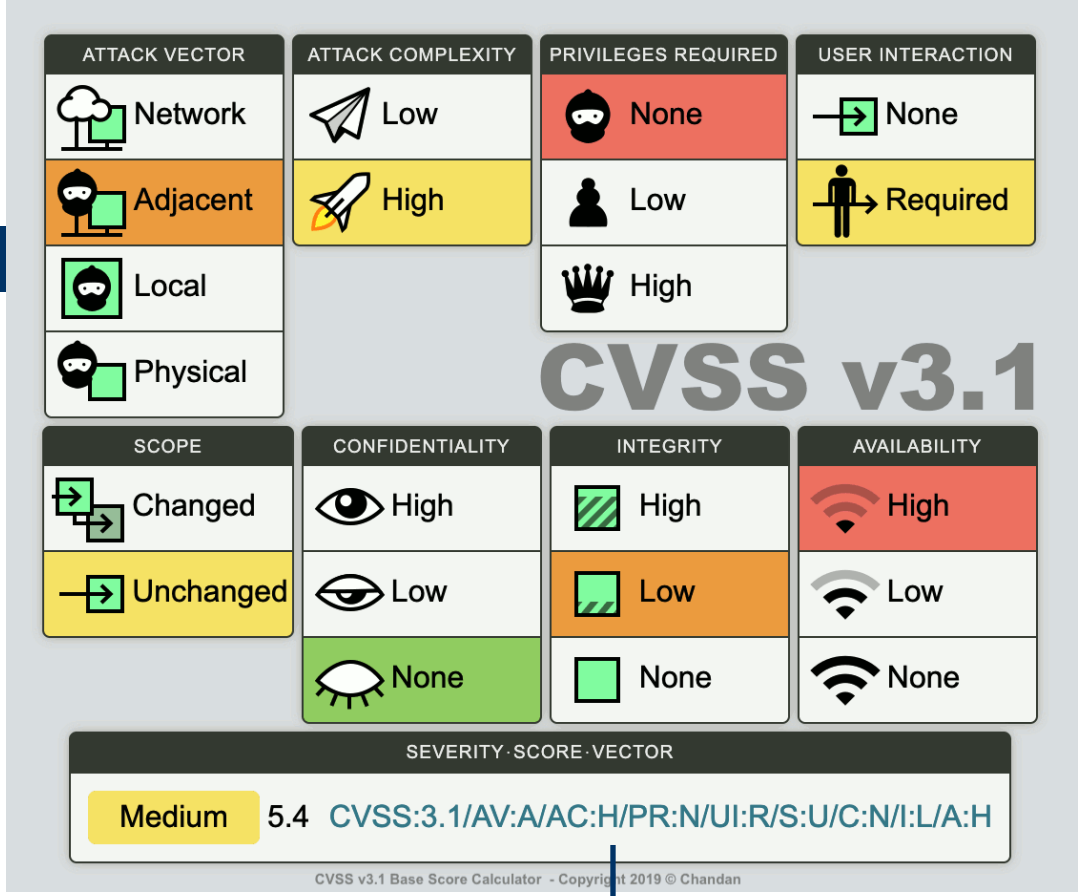
CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

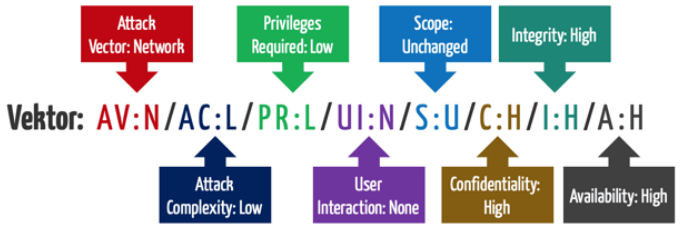


NVD

Definición

Severity Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 – 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 – 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 – 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMA-TIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.





AV: A AC:H PR:N UI:R S:U C:N I:L A:H

NVD

Definición

NVD Dashboard

CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	0	104	0	17
This Week	0	267	0	32
This Month	947	1144	0	135
Last Month	4085	3185	0	356
This Year	5032	4329	0	491

CVE Status Count

Total	280853
Received	297
Awaiting Analysis	22671
Undergoing Analysis	967
Modified	229348
Rejected	14773

NVD Contains

CVE Vulnerabilities	280853
Checklists	824
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	0
CPE Names	1367272

CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	24927
HIGH	66458
MEDIUM	67587
LOW	2807

CVSS V2 Score Distribution

Severity	Number of Vulns
HIGH	56836
MEDIUM	104167
LOW	19074

Resumen

Ideas principales

Sesión

Resumen

Ideas principales

Quien hace el resumen de este tema?

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652