UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Máster Universitario en Ingeniería Informática

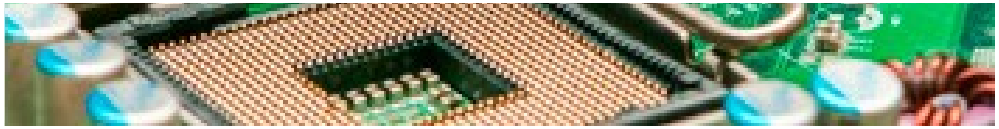
2022

CyberSeguridad
Tema 1: Vulnerabilidades

José Ismael Ripoll Ripoll

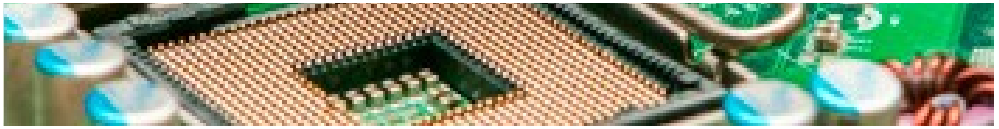
Máster Oficial Universitario en Ingeniería Informática
muiinf.webs.upv.es

MUIInf



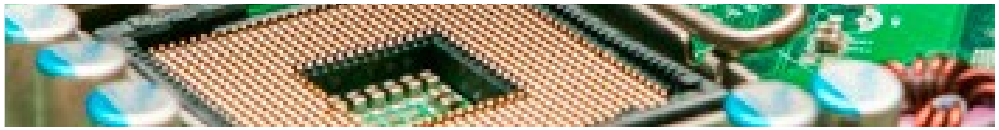
Contenidos

- Introducción y Terminología
- Debilidades
- Vulnerabilidades
- Alertas



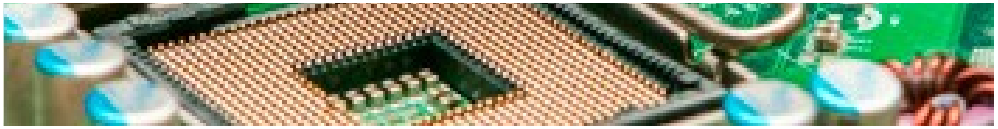
Conceptos y definiciones

- **Weakness**: (Debilidad) es un defecto o fallo de software, que *facilita* el ataque.
  - Pasword débil, no disponer de un firewall, debordamiento,…
- **Vulnerability**: (Agujero de seguridad) Es una debilidad que permite a un atacante violar se seguridad de un sistema. In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. [WP]
- **Asset**: (Bien, Activo) elemento de valor, tanto tangible como intangible.
- **PoC**: Proof of Concept or a Proof of Principle is a realization of a certain method or idea to demonstrate its feasibility. [WP]



Conceptos y definiciones

- **Stakeholder**: quienes son afectados o pueden ser afectados por las actividades de una empresa.
  - Todos aquellos agentes que de alguna forma tienen relación (influencian o son influenciados) por una actividad empresarial.
- **Target**: (objetivo) el bien que es objecto de un ataque.
- **Alert/Advisory**: Informe emitido por un fabricante o por una entidad de gestión de incidentes que pone de manifiesto un fallo en uno de sus productos.
- **Exploit**: A program or system designed to take advantage of a particular error or security vulnerability in computers or networks. [FreeDict]



¿Qué es una *weakness*?

§ **Software weaknesses**: are

flaws, faults, bugs, and other errors

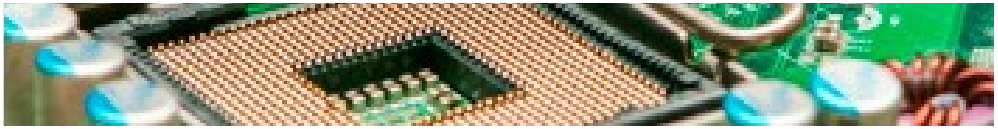
in

software implementation, code, design, or architecture

that if left unaddressed

could result in systems and networks being vulnerable to attack.

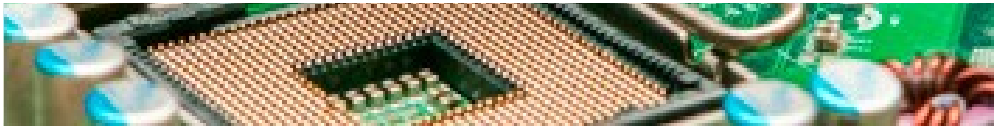
Example software weaknesses include: buffer overflows, format strings, etc.; structure and validity problems; common special element manipulations; channel and path errors; handler errors; user interface errors; pathname traversal and equivalence errors; authentication errors; resource management errors; insufficient verification of data; code evaluation and injection; and randomness and predictability.



Vulnerabilidad vs. Debilidad

- Software **weaknesses** are **errors that can lead to** software vulnerabilities.
- A software **vulnerability**, such as those enumerated on the Common Vulnerabilities and Exposures (CVE®) List, **is a mistake in software that can be directly used by a hacker** to gain access to a system or network.
- El MITRE ha recopilado una lista de unas 2000 debilidades diferentes.

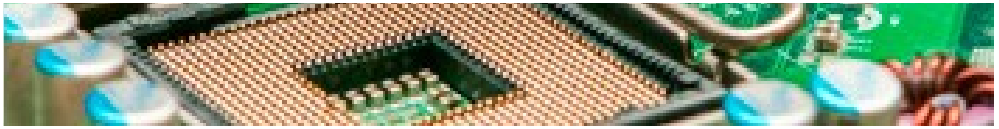
Weakness
es una generalización/abstracción de las **vulnerabilidades**.



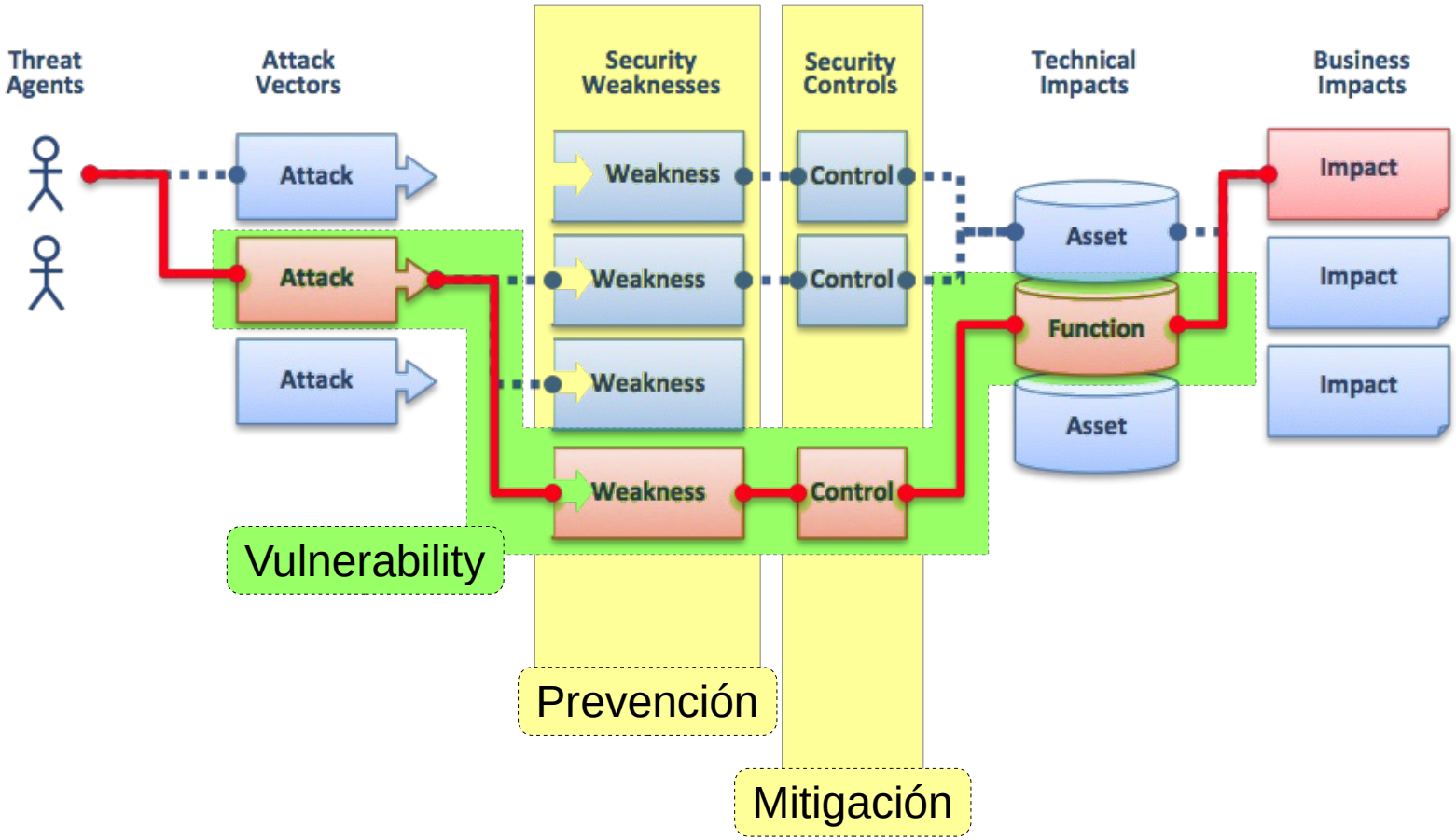
What is a vulnerability?

- System vulnerability is defined to be the intersection of:
  - **The fault**: System Susceptibility - The capacity of a system to be affected by a threat.
  - **The error**: Access to the flaw - The ability of a threat to gain access to a system, either physically or logically (e.g. over the network).
  - **The discovery**: Capability to exploit the flaw - The ability of the threat to employ the knowledge and tools necessary to exploit the system to achieve the desired goal.

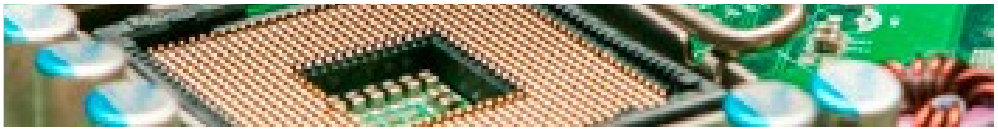
A fault without a PoC is not a vulnerability.
You must build an **exploit** to demonstrate that a vulnerability exists!



Vulnerability

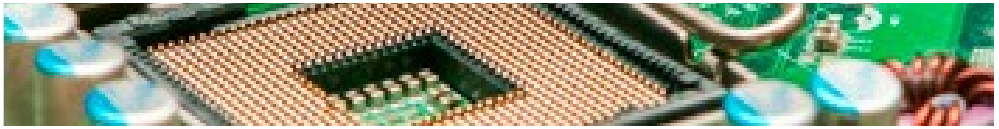


Source: Wikipedia



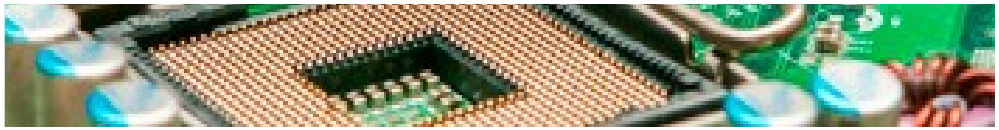
Soft error vs. vulnerability

- Most programming faults are not vulnerabilities.
- Only if the **assets** are jeopardised!
  - Access to privileged data.
  - Remote control.
  - System modification.
  - Service disruption.
- Han habido fallos que no se han sabido explotar durante muchos años, hasta que se descubrió la weakness:
  - Format String vulnerability.



Listado de Debilidades: CWEs

- Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weakness types that have security ramifications.
- Aunque dice que es community-developed, realmente lo gestiona el MITRE:
- https://cwe.mitre.org/about/index.html
- En la version 4.2 (2022) hay hasta CWE-1386:
  - https://cwe.mitre.org/data/archive.html



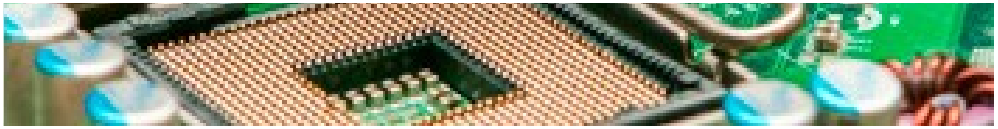
Top 25 CWE/SANS

- **SANS**: es un instituto de seguridad dedicado a la divulgación y la certificación.
- Colabora con el MITRE en la elaboración de la lista de las 25 debilidades más "**peligrosas**":

  "**CWE/SANS Top 25 Most Dangerous Software Errors**"

  - https://www.sans.org/top25-software-errors/ (Nuevo en 2022)
  - La ordenación tiene en cuenta el grado de peligrosidad individual y el número de incidentes registrados.
- También elaboran la lista:

  "Critical Security Controls"



§ CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

- http://cwe.mitre.org/top25/#CWE-89

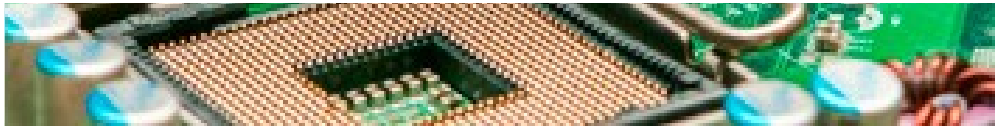
1 **CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Summary

Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

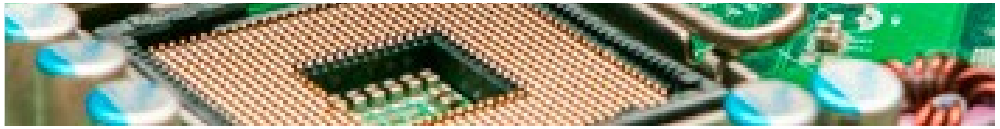
Discussion

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know how



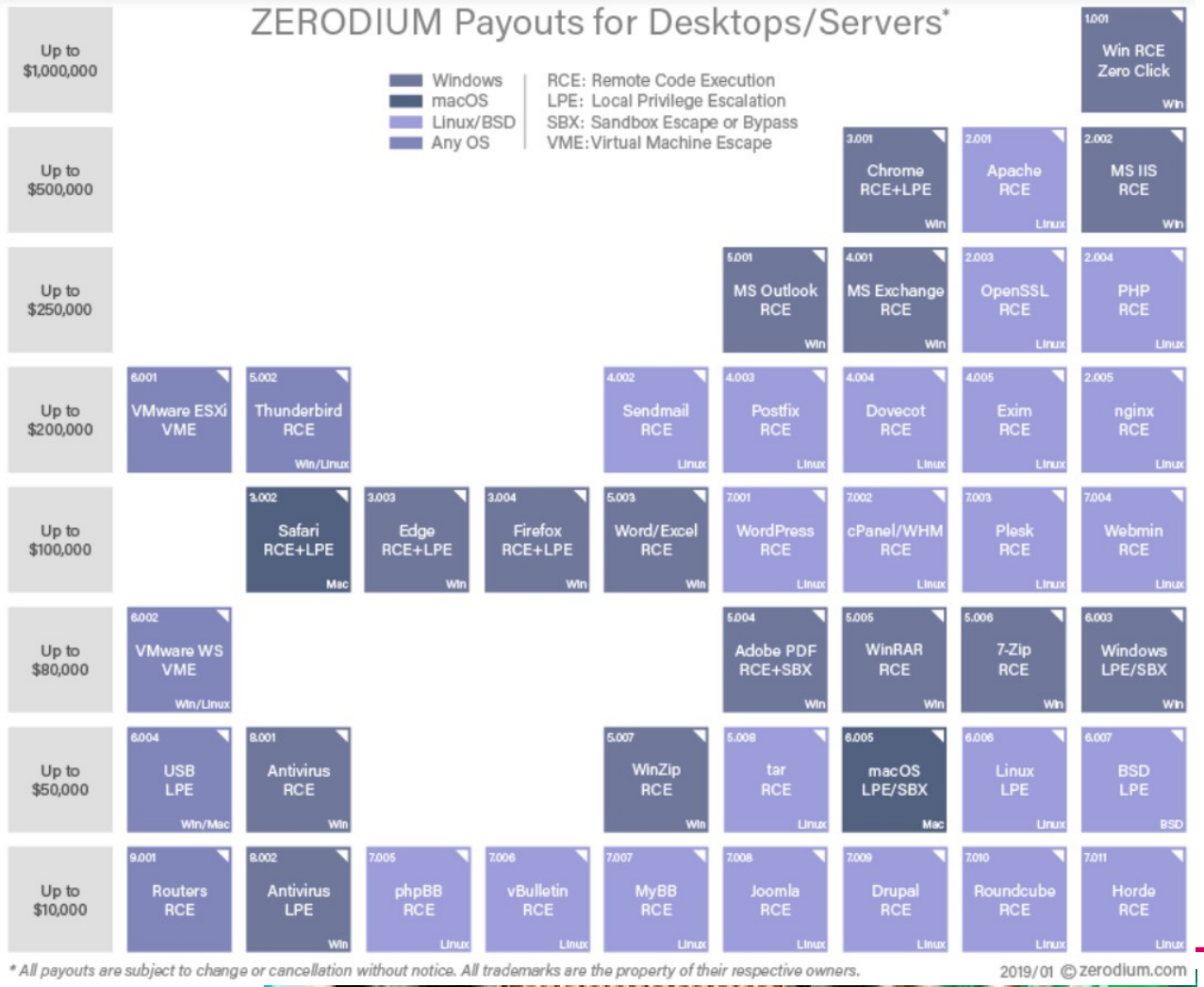
Listado de Vulnerabilidades: CVE

- CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." https://www.cvedetails.com/cve-help.php
- Por tanto "un CVE" es un identificador de una vulnerabilidad concreta.
- El identificador sigue el siguiente formato:
  - CVE-XXXX-YYYYY (XXXX→ Año, YYYYY → Número)



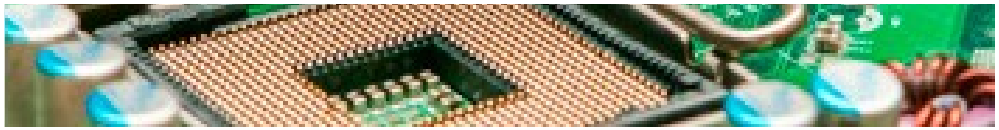
¿Cuanto vale una vulnerabilidad?

- En el mercado blanco… mucho
  - Zerodium
  - HakerOne
- En el negro++



Los bounty programs

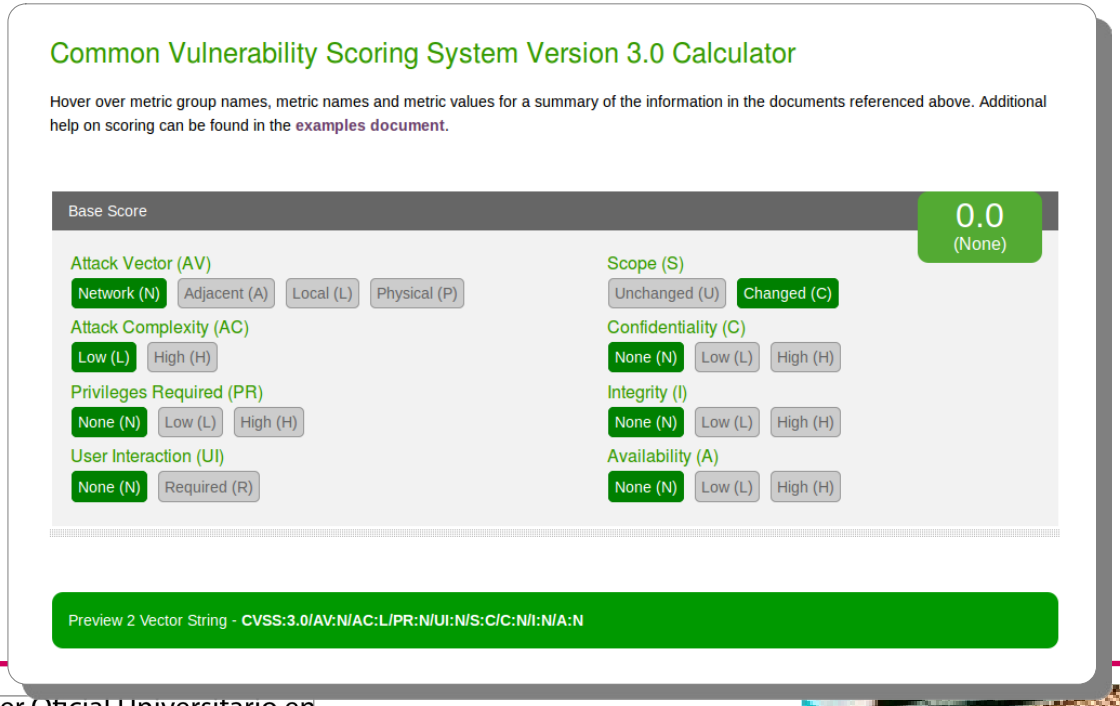
- Los principales fabricantes de software suelen tener programas de recompensas donde compran los fallos que los investigadores van descubriendo. También hay concursos o grupos especializados.
- Pwn2Own
  - Pwn2Own is a computer hacking contest held annually at the CanSecWest security conference
- Google Project Zero
  - Formed in 2014, Project Zero is a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world. Our mission is to make the discovery and exploitation of security vulnerabilities more difficult, and to significantly improve the safety and security of the Internet for everyone.



Métricas de vulnerabilidades: CVSS

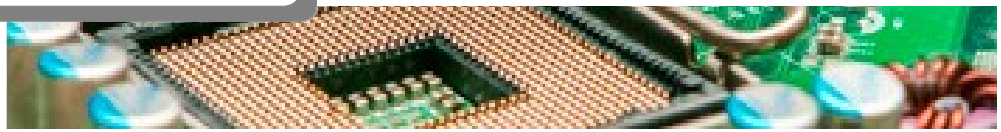
§ CVSS (Common Vulnerability Scoring System)

- Es un framework abierto que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad IT.
- Propuesto por : FIRST (Forum of Incident Response and Security Teams) https://www.first.org/cvss/calculator/3.0



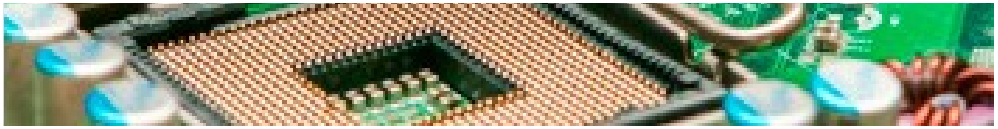
Si no afecta a la:
1.- **confidencialidad** ni a la
2.- **integridad** ni a la
3.- **disponibilidad**,

NO es una vulnerabilidad



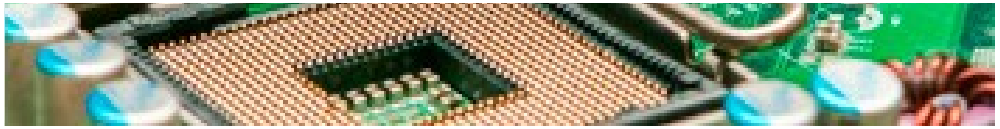
Organización de la identificación

- Se puede notificar al MITRE con un email sobre una vulnerabilidad identificada.
  - Breve descripción
- O se puede solicitar a una CNA
  - CVE Numbering Authorities
  - https://cve.mitre.org/cve/cna.html
- Si el MITRE no responde a la solicitud de identificador, entonces se puede utilizar otro servicio: OSVDB (http://osvdb.org)
  - Open Source Vulnerability Database.
  - Son menos estrictos a la hora de calificar como vulnerabilidades ciertos fallos.

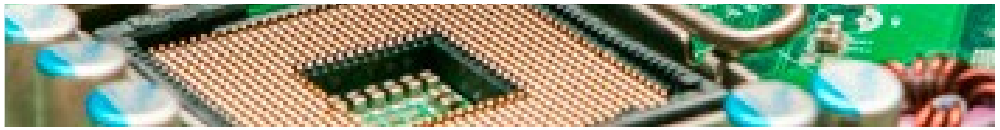


Alerts/Advisories

- Los principales fabricantes de SW publican notas de seguridad para alertar a los clientes de las vulnerabilidades que se deben resolver.
- Cada fabricante numera los advisories siguiendo su propia nomenclatura:
  - Microsoft: **MSyy-XXX**
  - Debian: **DSA-XXXX-X**
  - CISCO: **cisco-sa-yyyymmdd-text**
  - Ubuntu: **USN-XXXX-X**
  - CERT: **Tayy-XXXX**
- **http://www.infosecindustry.com/#Alerts**

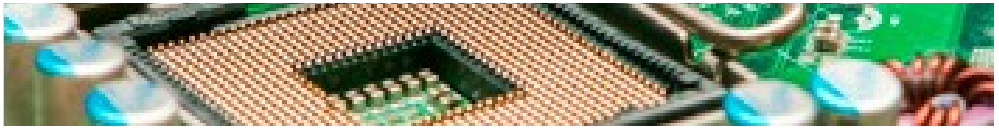


- OWASP: es una organización internacional que trata de ayudar para que la red sea más segura.
  - Desarrolla documentación muy buena.
- OWASP Top 10:
  - A list of the 10 Most Critical Web Application Security Risks.
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Excelente sitio con libros sobre desarrollo web EXCELENTES.



A recordar

- **CWE**: Listado de debilidades.
- **CVE**: Listado de vulnerabilidades.
- **CVSS**: Métrica para calibrar el impacto de una vulnerabilidad o debilidad.
- **OWASP**: Open Web Application Security Project is a worldwide not-for-profit charitable organization focused on improving the security of software.



Links

- https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/cvss3_0
- https://en.wikipedia.org/wiki/Vulnerability_%28computing%29
- https://cwe.mitre.org/cwss/cwss_v1.0.1.html
- https://cwe.mitre.org/about/faq.html
- https://www.owasp.org/index.php/Main_Page