U4 – Gestión de Vulnerabilidades Seguridad

Mg. Ing. Bruno Roberti

2.023

Vulnerabilidad de Seguridad

Vulnerabilidad de Seguridad

Es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema de información, que puede ser explotado por una o mas amenazas, con el fin de comprometer la seguridad del sistema.

Amenaza

Acción que puede ocurrir y aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

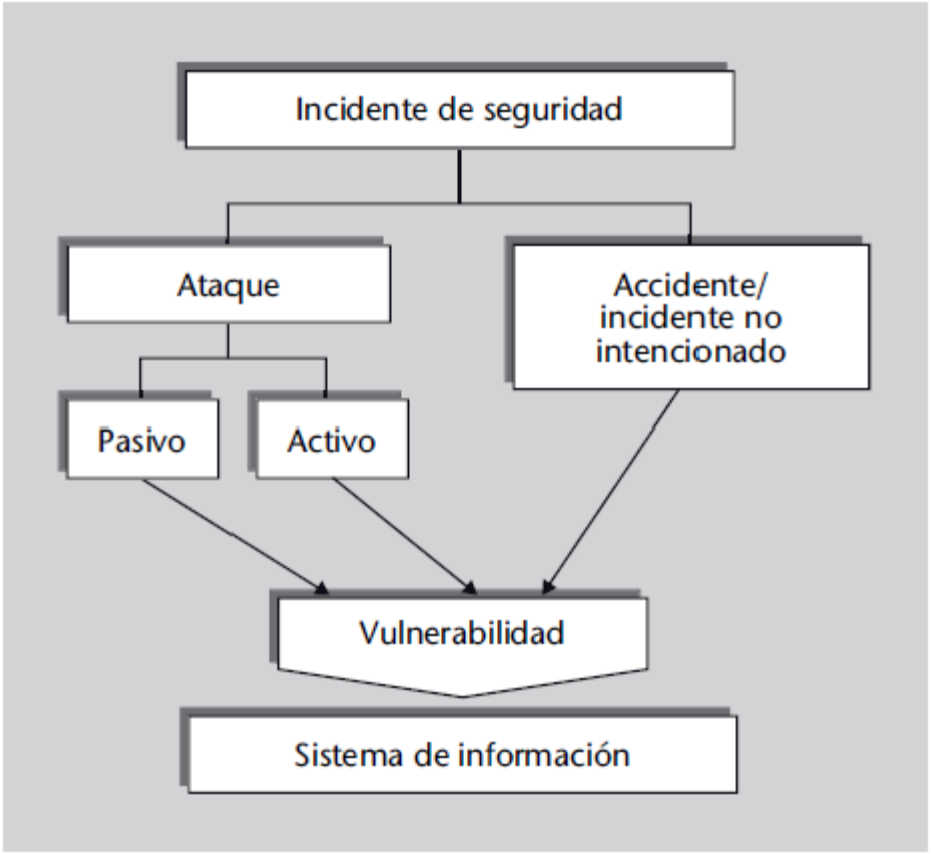
Incidente

El incidente es la materialización de una amenaza. Evento Adverso que afecta al funcionamiento del sistema informático

Ataque

Agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema.

Relación entre incidentes, amenazas y vulnerabilidades



Perfil del atacante

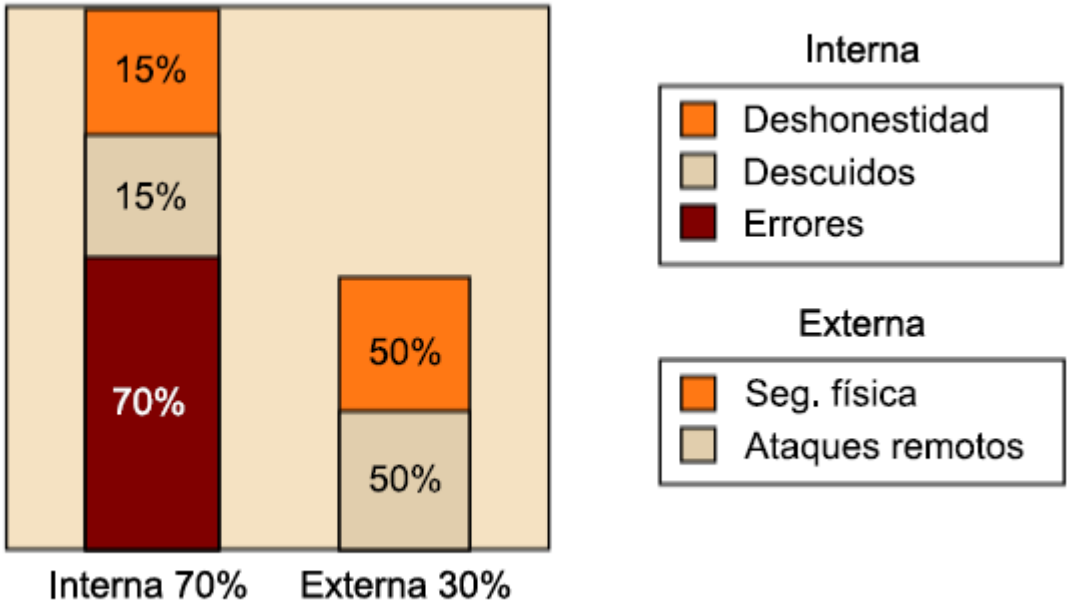
Internos

Antiguos trabajadores: Una parte muy importante de los ataques a sistemas informáticos son los realizados por antiguos trabajadores que, antes de dejar la organización,

Personal de la misma organización: Algunos ataques se pueden producir desde dentro mismo de la institución. A menudo, no hace falta que estos ataques sean intencionados.

Externos

- Hackers
- Criminales



Porcentaje y tipo de ataques en una organización. (Fuente http://www.cybsec.com)

Etiquetado de Vulnerabilidades

CVE (Common Vulnerabilities and Exposures).

El sistema de identificación más importante a escala internacional.

https://www.cve.org/

CVE ID: CVE + AÑO + NRO

- **NRO= arbitrario mayor a 4 dígitos**

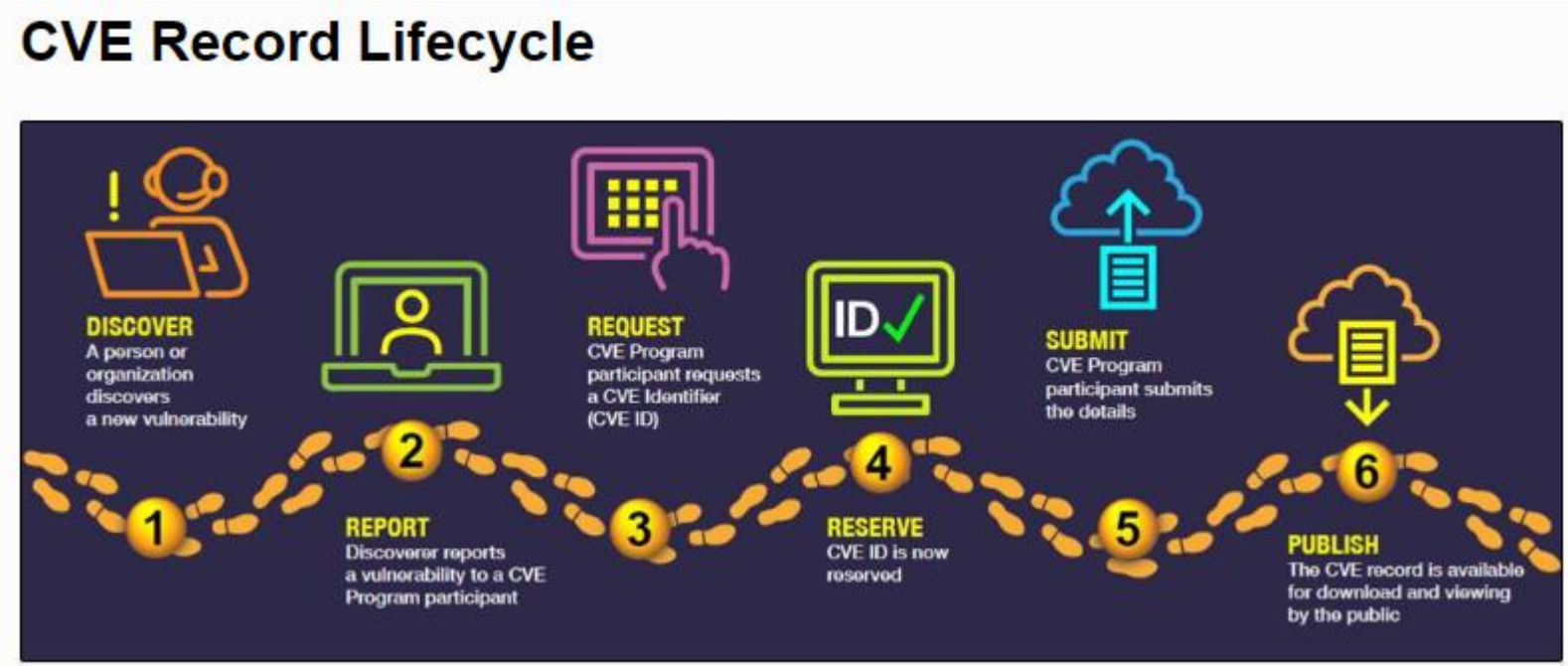
Registro CVE: CVE ID + Descripción + Referencias

- Ejemplo: https://www.cve.org/CVERecord?id=CVE-2017-2641

Estado Registro CVE:

- Reservado / Publicado / Rechazado

Etiquetado de Vulnerabilidades



Persona u Organización

Miembro del programa (Root; CNA, etc)

CVE Numbering Authorities

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523

CVE-ID

CVE-2011-2523 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:[oss-security] 20110711 Re: vsftpd download backdoored
- URL:https://www.openwall.com/lists/oss-security/2011/07/11/5
- MISC:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html
- URL:http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html
- MISC:https://access.redhat.com/security/cve/cve-2011-2523
- URL:https://access.redhat.com/security/cve/cve-2011-2523
- MISC:https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html
- URL:https://packetstormsecurity.com/files/102745/VSFTPD-2.3.4-Backdoor-Command-Execution.html
- MISC:https://security-tracker.debian.org/tracker/CVE-2011-2523
- URL:https://security-tracker.debian.org/tracker/CVE-2011-2523
- MISC:https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805
- URL:https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805

Assigning CNA

Red Hat, Inc.

Date Record Created

20110615 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20110615)

Votes (Legacy)

https://www.exploit-db.com/exploits/49757

https://nvd.nist.gov/vuln/detail/CVE-2011-2523

VULNERABILITIES

CVE-2011-2523 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2011-2523
NVD Published Date:
11/27/2019
NVD Last Modified:
04/12/2021
Source:
Red Hat, Inc.

Evaluación de Vulnerabilidades

CVSS (Common Vulnerability Scoring System)

El sistema de evaluación más extendido a nivel mundial.

https://www.first.org/cvss/specification-document

Métrica Base

- Aspectos de la vulnerabilidad constantes en el tiempo y entorno

Métrica Temporal

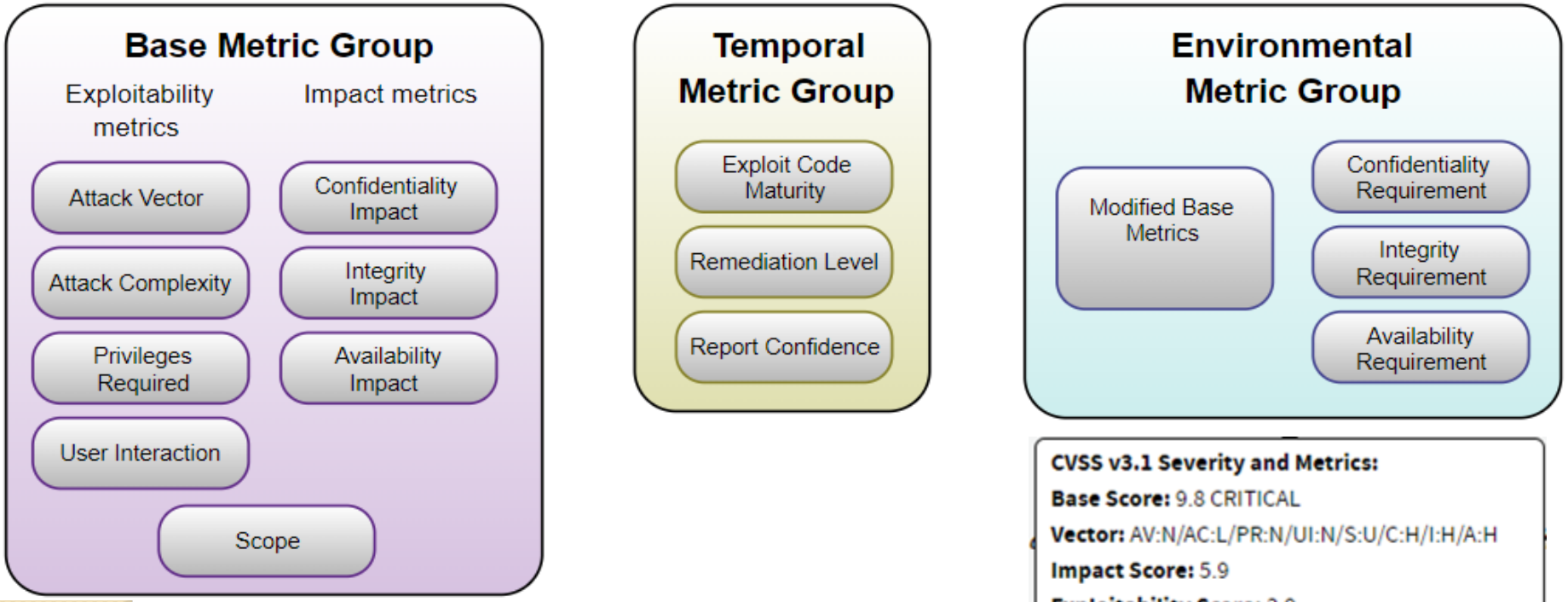
- Aspectos que pueden cambiar en el tiempo.

Métrica de Entorno

- Métricas relativas al entorno del sistema informático propiamente dicho

Evaluación de Vulnerabilidades

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure 1.



Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High