



Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

Maestría en ciberseguridad y ciberdefensa



El futuro
es de todos

Presidencia
de la República



LA VICTORIA ES
DE TODOS
FUERZAS MILITARES DE COLOMBIA



Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

Gestión del Riesgo Cibernético

Ing. Jaider Ospina Navas, M.Sc.



El futuro
es de todos

Presidencia
de la República



LA VICTORIA ES
DE TODOS
FUERZAS MILITARES DE COLOMBIA

Métricas de evaluación de vulnerabilidades: CVSS 3.1 (Common Vulnerability Score System)



Common Vulnerability Score System (CVSS) sistema de puntaje que provee un método abierto y estándar que permite **estimar el impacto** de vulnerabilidades.

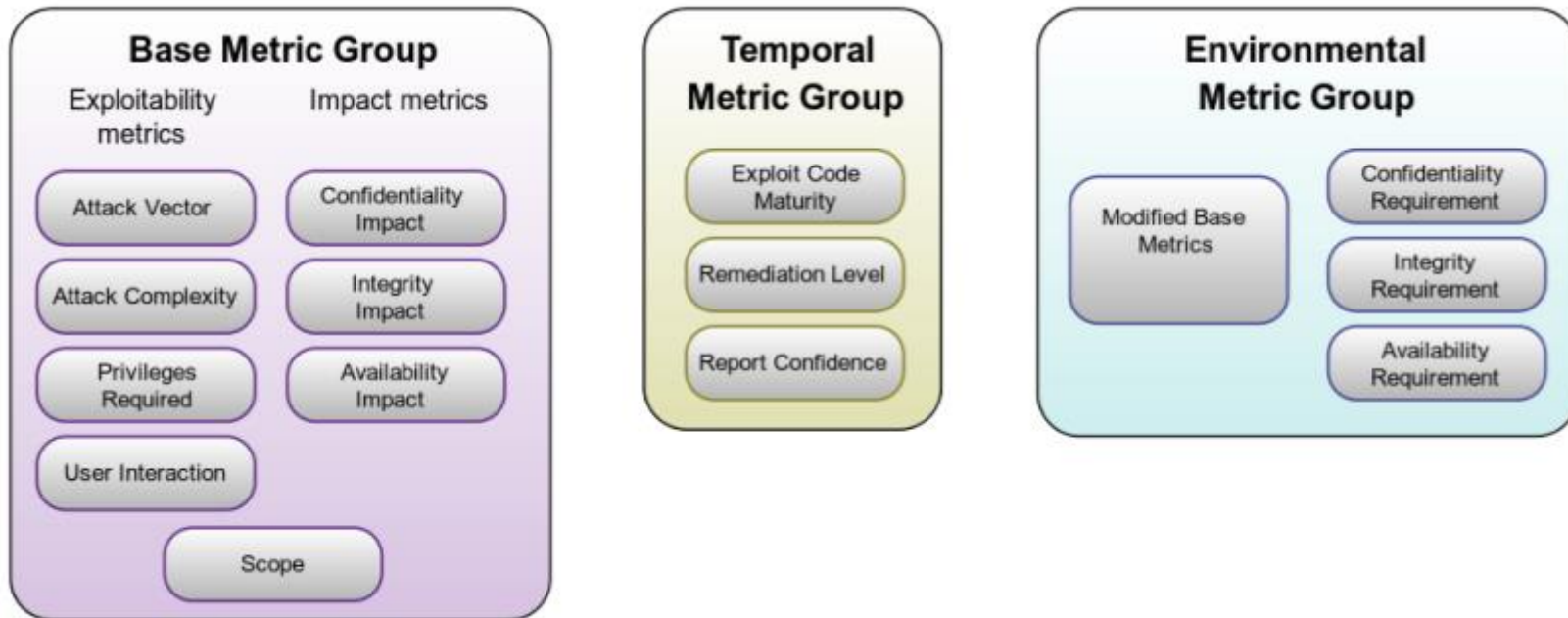
Forum of Incident Response and Security Teams (FIRST).

- Framework open.



Empleado por bases de datos de vulnerabilidades públicamente conocidas como: *National Vulnerability Database* ([NVDB](#)), *Common Vulnerabilities and Exposures* ([CVE](#)) y *Open Source Vulnerability Database* ([OSVDB](#)).

Grupos de Métricas



Fuente: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

CVSS V3

GRUPO DE MÉTRICAS BASE

Métrica de explotabilidad

- ✓ Vector de ataque
- ✓ Complejidad del ataque
- ✓ Privilegios requeridos
- ✓ Interacción con el usuario

Métricas de impacto

- ✓ Impacto en la confidencialidad
- ✓ Impacto en la integridad
- ✓ Impacto en la disponibilidad

✗ Puntuación

CVSS V4

GRUPO DE MÉTRICAS BASE

Métrica de explotabilidad

- ✓ Vector de ataque
- ✓ Complejidad del ataque
- ¡Nuevo! Requisitos de ataque
- ✓ Privilegios requeridos
- ✓ Interacción con el usuario

Impact Metrics

- ✓ Confidencialidad del sistema vulnerable
- ✓ Integridad del sistema vulnerable
- ✓ Disponibilidad del sistema vulnerable
- ¡Nuevo! Confidencialidad del sistema posterior
- ¡Nuevo! Integridad del sistema posterior
- ¡Nuevo! Disponibilidad del sistema posterior



Componente Existente



Componente Existente con cambios



Retirado del CVSS en la V4



Nuevo Componente en la V4

Grupo Base: Engloba las cualidades intrínsecas de una vulnerabilidad y que son independientes del tiempo y el entorno. Las métricas evaluadas en este grupo son:

- **Access Vector (AV).** Valores: [L,A,N] (Local, Adjacent, Network).
- **Access Complexity (AC).** Valores [H,M,L] (High, Medium, Low).
- **Authentication (Au).** Valores [M,S,N] (Multiple, Single, None).
- **Confidentiality Impact (C)** . Valores [N,P,C] (None, Partial, Complete).
- **Integrity Impact (I).** Valores [N,P,C] (None, Partial, Complete).
- **Availability Impact (A).** Valores [N,P,C] (None, Partial, Complete)

Grupo Temporal: Características de la vulnerabilidad que cambian en el tiempo. Se aplican tres métricas:

- **Exploitability (E).** Valores: [U,POC,F,H,ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined).
- **Remediation Level (RL).** Valores: [OF,TF,W,U,ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined).
- **Report Confidence (RC).** Valores: [UC,UR,C,ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined)

Grupo Environmental: Las características de la vulnerabilidad relacionadas con el entorno del usuario. En este caso los factores que se evalúan son:

- **Collateral Damage Potential (CDP).** Valores: [N,L,LM,MH,H,ND] (None, Low, Low Medium, Medium High, High, Not Defined).
- **Target Distribution (TD).** Valores: :[N,L,M,H,ND] (None, Low, Medium, High, Not Defined).
- **Security Requirements (CR, IR, AR).** Valores: [L,M,H,ND] (Low, Medium, High, Not Defined)

Principales cambios de CVSS 3.1 respecto a CVSS 3.0

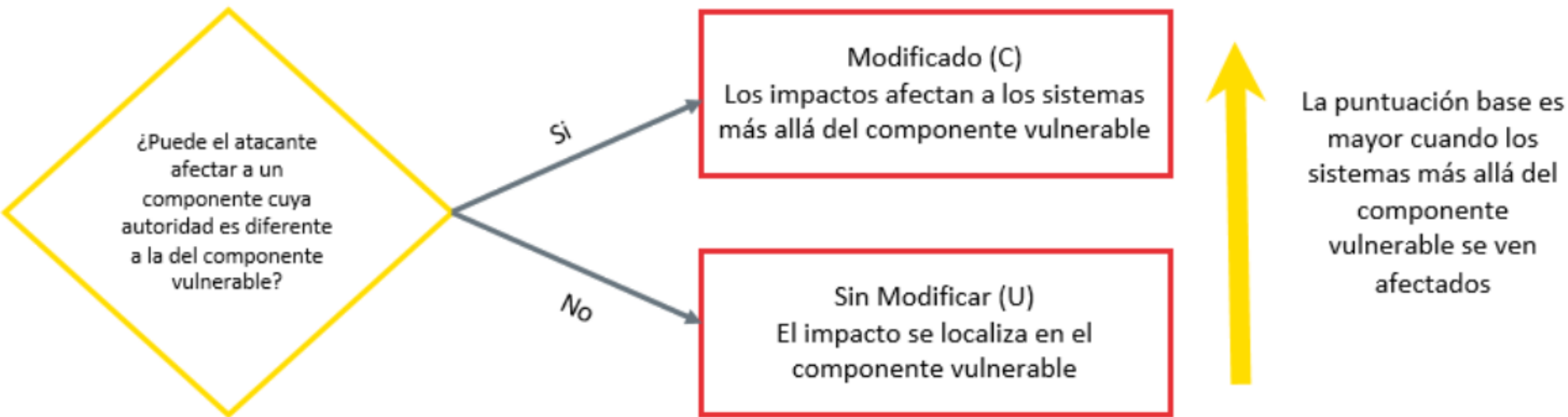
CVSS mide la gravedad, no el riesgo

- CVSS (*Base Score*) representa sólo las **características intrínsecas** de una vulnerabilidad que son constantes en el tiempo y son comunes a los distintos entornos de usuario.
- Para llevar a cabo un análisis de riesgos sistemático, esta puntuación base debe complementarse con un análisis contextual aprovechando las métricas temporales y del entorno, y con otros factores externos no contemplados por el CVSS como exposición y amenaza.

Principales cambios de CVSS 3.1 respecto a CVSS 3.0

- CVSS (Base Score) representa sólo las características intrínsecas de una vulnerabilidad que son constantes en el tiempo y son comunes a los distintos entornos de usuario.
- Para llevar a cabo un análisis de riesgos sistemático, esta puntuación base debe complementarse con un análisis contextual aprovechando las métricas temporales y del entorno, y con otros factores externos no contemplados por el CVSS como exposición y amenaza.
- En la nueva versión se ha incluido una nueva métrica denominada 'alcance', debido a que existen vulnerabilidades que pueden identificarse en un **componente específico** (componente vulnerable), pero que sin embargo pueden afectar a otros elementos (componente impactado).

Se reformulan para aclararlos, la explicación de la métrica *Scope* del documento de especificaciones y los conceptos de *Vulnerable Component* (elemento que es vulnerable) e *Impacted Component* (elemento que sufre el impacto). Se añade un apartado en la guía de usuario con ejemplos.



Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of a calculator (including its design and an XML representation for CVSS v3.1).

Base Score

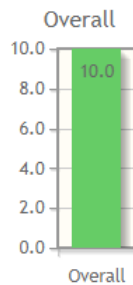
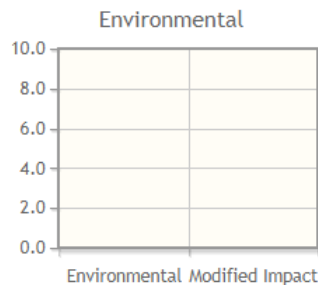
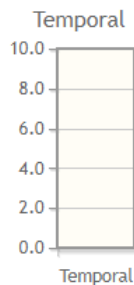
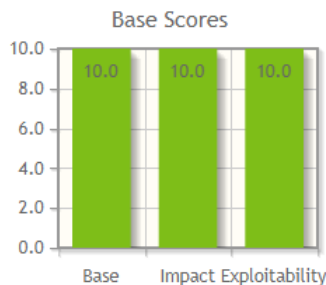
Attack Vector (AV)	Scope (S)
<input type="button" value="Network (N)"/> <input type="button" value="Adjacent (A)"/> <input type="button" value="Local (L)"/> <input type="button" value="Physical (P)"/>	<input type="button" value="Unchanged (U)"/> <input type="button" value="Changed (C)"/>
Attack Complexity (AC)	Confidentiality (C)
<input type="button" value="Low (L)"/> <input type="button" value="High (H)"/>	<input type="button" value="None (N)"/> <input type="button" value="Low (L)"/> <input type="button" value="High (H)"/>
Privileges Required (PR)	Integrity (I)
<input type="button" value="None (N)"/> <input type="button" value="Low (L)"/> <input type="button" value="High (H)"/>	<input type="button" value="None (N)"/> <input type="button" value="Low (L)"/> <input type="button" value="High (H)"/>

<https://www.first.org/cvss/>

Common Vulnerability Scoring System Calculator - CVE-2014-6271

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 10.0

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Temporal Score: NA

CVSS Environmental Score: NA

Modified Impact Subscore: NA

Overall CVSS Score: 10.0












Show Equations












CVSS v2 Vector

(AV:N/AC:L/Au:N/C:C/I:C/A:C)

<https://nvd.nist.gov/vuln/search>

CVSS v3.1 Base Score Calculator

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
 Network	 Low	 None	 None
 Adjacent	 High	 Low	 Required
 Local		 High	
 Physical			

SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
 Changed	 High	 High	 High
 Unchanged	 Low	 Low	 Low
	 None	 None	 None

SEVERITY SCORE VECTOR

High 7.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

Copyright 2019 © Chandan
 CVSSjs is free to use, copy, modification under a BSD like licence.
 Common Vulnerability Scoring System (CVSS) is a free and open standard. It is owned and managed by FIRST.Org.

Fuente: <https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H>

3. MySQL Stored SQL Injection (CVE-2013-0375)

Vulnerability

A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that runs with high privileges on a remote MySQL Server database. A successful attack could allow any data in the remote MySQL database to be read or modified. The vulnerability occurs due to insufficient validation of user-supplied data as it is replicated to remote MySQL Server instances.

Attack

An attacker requires an account on the target MySQL database with the privilege to modify user-supplied identifiers, such as table names. The account must be on a database which is configured to replicate data to one or more remote MySQL databases. An attack consists of logging in using the account and modifying an identifier to a new value that contains a quote character and a fragment of malicious SQL. This SQL will later be replicated to, and executed on, one or more remote systems, as a highly privileged user. The malicious SQL is injected into SQL statements in a way that prevents the execution of arbitrary SQL statements.

EJEMPLO

CVSS v2.0 Base Score: 5.5

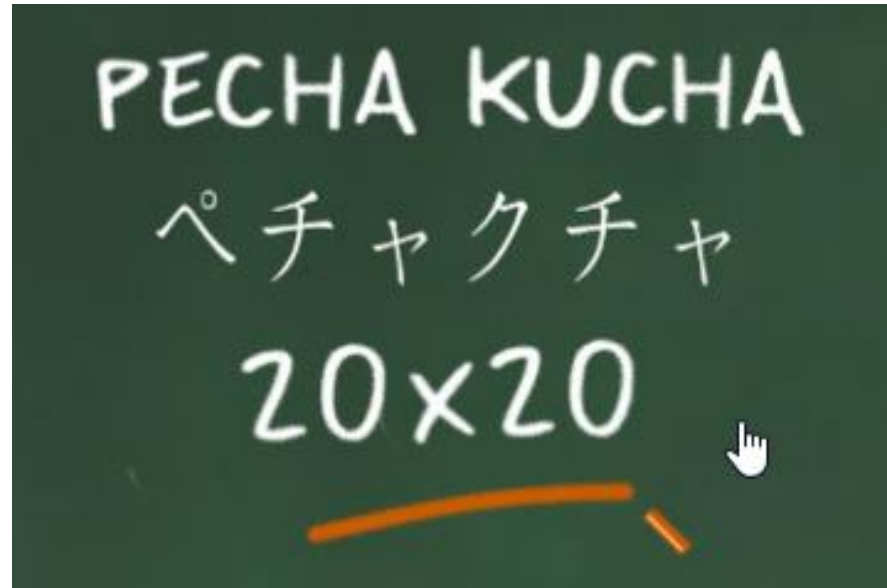
Metric	Value
Access Vector	Network
Access Complexity	Low
Authentication	Single
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS v3.1 Base Score: 6.4

Metric	Value	Comments
Attack Vector	Network	The attacker connects to the exploitable MySQL database over a network.
Attack Complexity	Low	Replication must be enabled on the target database. Following the guidance in Section 2.1.2 of the Specification Document that was added in CVSS v3.1, we assume the system is configured in

Privileges Required	Low	The attacker requires an account with the ability to change user-supplied identifiers, such as table names. Basic users do not get this privilege by default, but it is not considered a sufficiently trusted privilege to warrant this metric being High.
User Interaction	None	No user interaction is required as replication happens automatically.
Scope	Changed	The vulnerable component is the MySQL server database that the attacker logs into to perform the attack. The impacted component is a remote MySQL server database (or databases) that this database replicates to.
Confidentiality	Low	The injected SQL runs with high privilege and can access information the attacker should not have access to. Although this runs on a remote database (or databases), it may be possible to exfiltrate the information as part of the SQL statement. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Integrity	Low	The injected SQL runs with high privilege and can modify information the attacker should not have access to. The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements.
Availability	None	Although injected code is run with high privilege, the nature of this attack prevents arbitrary SQL statements being run that could affect the availability of MySQL databases.

TECNICAS GERENCIALES



<https://prezi.com/yrcavugk1om8/pecha-kucha/>

Taller

https://www.first.org/cvss/v3-1/cvss-v31-examples_r1.pdf

- Del apartado de ejemplos del FIRST tome un ejemplo y realice una presentación tipo pechakucha (**3 diapositivas** sólo) con cualquier herramienta que le sea fácil de manejar (Powerpoint, Impress, Prezi, Canva, Emaze, Genial.ly, Powtoon, etc.) en el que se presente la descripción de la vulnerabilidad descrita:

1. Describa tanto el sistema, servicio o protocolo Vulnerable.
2. La técnica de explotación.
3. La descripción de catalogación de los diferentes componentes del score base.

Lista pública de fallas de seguridad informática que se encuentra disponible al público.

Permiten que los especialistas en TI coordinen sus esfuerzos para priorizar y solucionar estos puntos vulnerables.



¿Cómo funciona el sistema de CVE?

CVE-2014-0160
(TLS- DTLS-OpenSSL)

Heartbleed

MITRE Corporation se encarga de supervisar los CVE con el financiamiento de la Agencia de Seguridad de Infraestructura y Ciberseguridad, que forma parte del Departamento de Seguridad Nacional de Estados Unidos.

No describen datos técnicos ni información sobre riesgos, efectos o soluciones. Ese tipo de información aparece en otras bases de datos, incluidas la National Vulnerability Database de Estados Unidos, la CERT/CC Vulnerability Notes Database y varias listas que mantienen los proveedores y demás empresas.

¿Cómo se asigna un número de identificación de CVE?

Una autoridad de numeración de CVE (CNA) es la encargada de asignar los números de identificación de CVE.

Estas representan a proveedores de TI, empresas de seguridad y de investigación; así como el mismo MITRE.

Una vez que se publica una entrada de CVE:

- Formato "CVE-YYYY-NNNN" CVE-2019-1234567".
- Una descripción breve de la exposición o el punto vulnerable de seguridad.
- Y referencias, que pueden contener enlaces a avisos e informes del punto vulnerable.

Los informes de CVE pueden provenir de cualquier persona como algún proveedor, investigador o particular. Muchos proveedores ofrecen recompensas por detectar fallas de seguridad.

¿Qué características debe tener una falla para que se la califique como CVE?

1. Se pueden solucionar de forma independiente.

La falla puede solucionarse independientemente de las demás.

2. El proveedor afectado las confirma.

O

Se han justificado. La persona que notificó compartió un informe de vulnerabilidad donde se demuestra que tiene un impacto negativo e infringe la política de seguridad del sistema afectado.

3. Afectan una base del código.

Las fallas que afectan más de un producto obtienen distintos CVE. En los casos de bibliotecas, protocolos o estándares compartidos, se asigna un solo CVE a la falla si no hay manera de utilizar el código compartido sin quedar expuesto al punto vulnerable. De lo contrario, se asigna un CVE única a cada producto o base de código afectados.

- CVE y NVD son programas separados.
- CVE es lanzado por MITRE en 1999.
- National Vulnerability Database (NVD), fué lanzado por el NIST (National Institute of Standards and Technology) en 2005.
- CVE alimenta a NVD, el cual clasifica y complementa la información (puntaje de gravedad, clasificación del impacto...), así como funciones de búsqueda por diferentes criterios (SO, proveedor, número de producto, etc).
- Ambas son patrocinadas por la Agencia de Ciberseguridad e Infraestructura (CISA) del Departamento de Seguridad Nacional de EE. UU. (DHS), y ambos están disponibles para el público y son de uso gratuito.



CVE
Common Vulnerabilities and Exposures

CVE List ▾

HOME > CVE LIST > CVE DATA FEEDS

CVE Data Feeds

Please see below for the latest CVE updates.

Newest CVE Entries Feed

Tweets by @CVEnew

CVE
@CVEnew
CVE-2020-1631 A vulnerability in the HTTP/HTTPS service used by J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Zero Touch Provi...
cve.mitre.org/cgi-bin/cvenam...

<https://cve.mitre.org/>

NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

General +
Vulnerabilities +
Vulnerability Metrics +
Products +
Configurations (CCE) +
Contact NVD +
Other Sites +
Search +

Other Sites
In addition to the many resou...
NCP Repository
800-53 Controls
SCAP Validated Tools

<https://nvd.nist.gov/products>

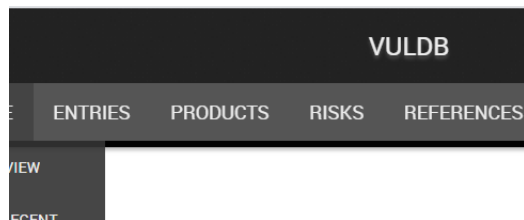
Bases de datos de Vulnerabilidades

Computer Incident Response Center Luxembourg. Se trata de una organización de seguridad diseñada para detectar y solucionar amenazas cibernéticas.



circl.lu
Computer Incident
Response Center
LUXEMBOURG

<https://circl.lu/mission/>



Base de datos de **CVE**. Calificadas bajo el riesgo del exploit encontrado: bajo, medio o alto.

IT Security Database

Vulnerability, patch and compliance datasource

[Home](#) [Help](#) [Search](#) [CVE Vulnerability Database](#)

Browse

[OVAL Objects](#)
[OVAL Sources](#)
[By Release Dates](#)

OVAL Definitions

[Windows](#)
[Compliance](#)
[Inventory](#)
[Patches](#)
[Vulnerabilities](#)
[Unix/Linux](#)
[Compliance](#)
[Inventory](#)
[Patches](#)
[Vulnerabilities](#)
[Red Hat Advisories](#)
[Suse Linux Advisories](#)
[IOS](#)
[PlixOS](#)

OVAL Classes

[Compliance](#)
[Inventory](#)
[Miscellaneous](#)
[Patch](#)
[Vulnerability](#)

Patch [oval.org.mitre.oval:def:23497](#)

ELSA-2012:0813: 389-ds-base security, bug fix, and enhance

[Dependent \(Extending\) Definitions](#) [View Definition At Mitre](#)

The aclas__handle_group_entry function in servers/plugins/acl/acllas.c in 389 Directory S remote authenticated LDAP users with a certificate group to cause a denial of service (infinite loop).
Create Date: 2014-01-13 Last Update Date: 2014-05-26

Affected Platforms/Products

Affected Products (CPE + CVE references)

- [Fedora project](#) [389 Directory Server](#)

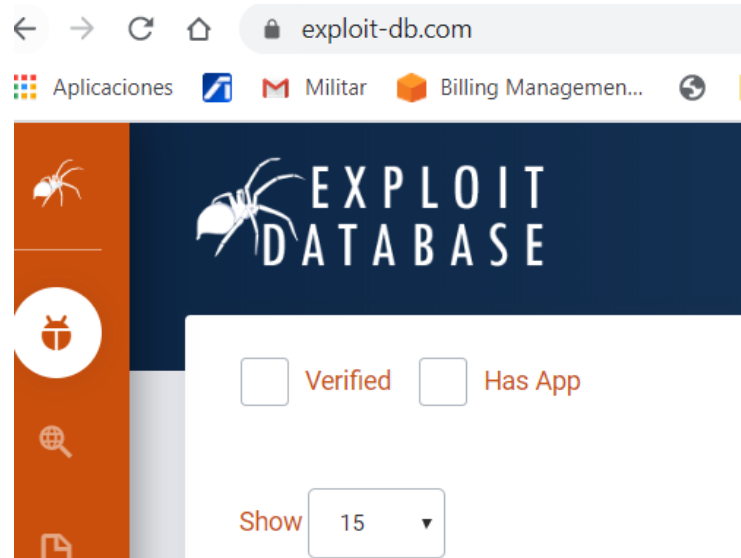
Platforms: [unix \(from OVAL definitions\)](#) Products: [unix](#)

- [Oracle Linux 6](#) [389-ds-base](#)

References

- VENDOR : [ELSA-2012:0813-04](#) <http://linux.oracle.com/errata/ELSA-2012-0813.html>
- [CVE-2012-0833](#)

<https://www.itsecdb.com/oval/>



<https://www.exploit-db.com/>



<https://www.rapid7.com/db/>

Open Vulnerability and Assessment Language (OVAL®)

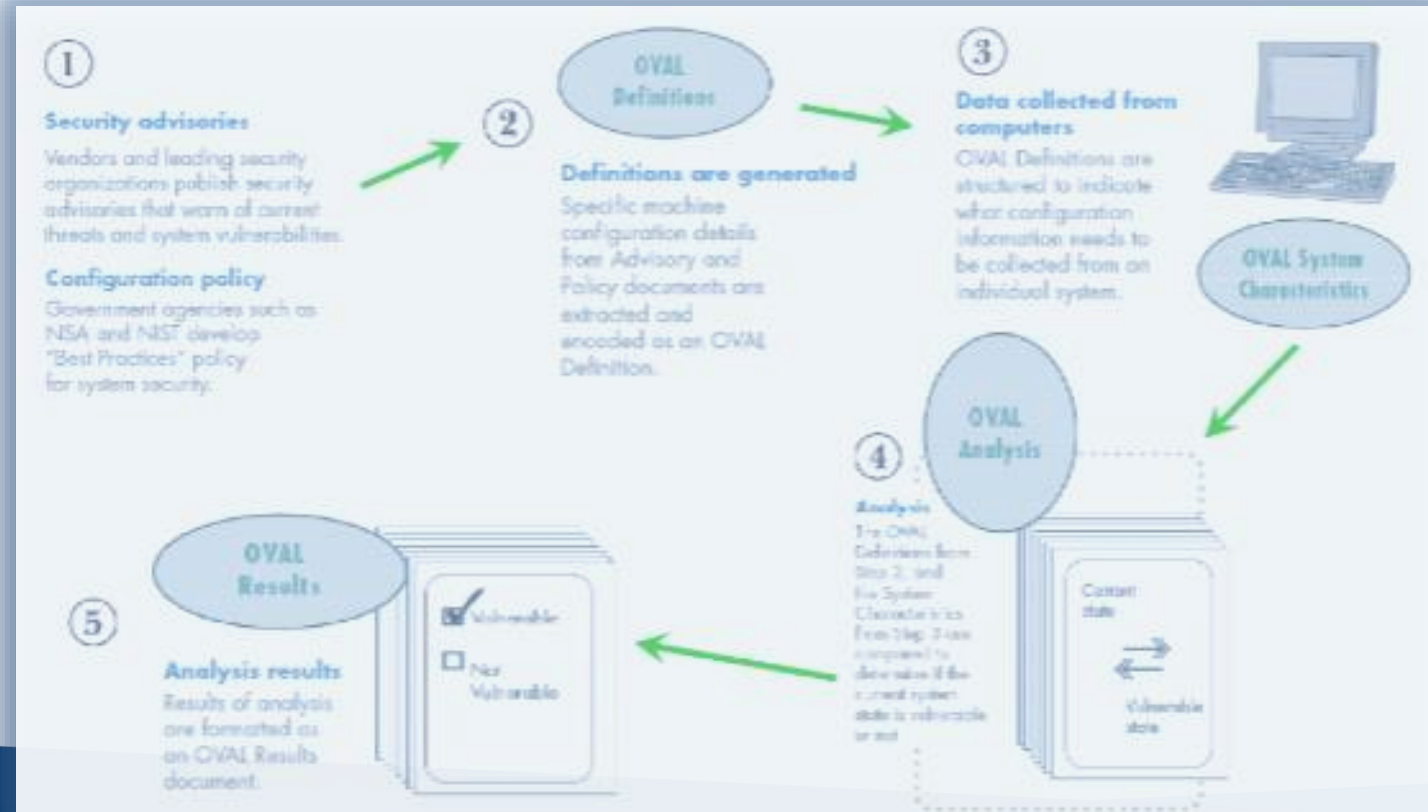


International in scope and free for public use, **OVAL®** is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

<https://oval.cisecurity.org/>

OVAl (Open Vulnerability Assessment Language) es una colección de esquemas XML para representar información de sistemas; expresando estados de máquinas específicos y reportando resultados de evaluación.





¿QUE QUÉ ELIJO?



YO lo tengo claro:

A

Repositorio de técnicas y procedimientos de ataques y defensas

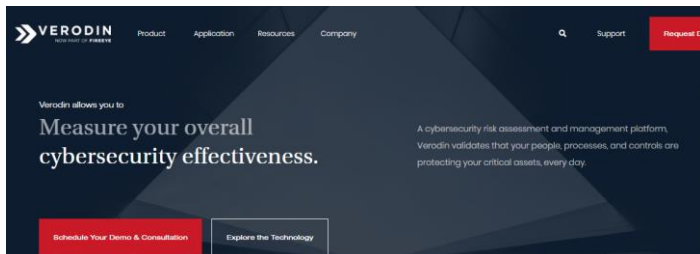
ATT&CK



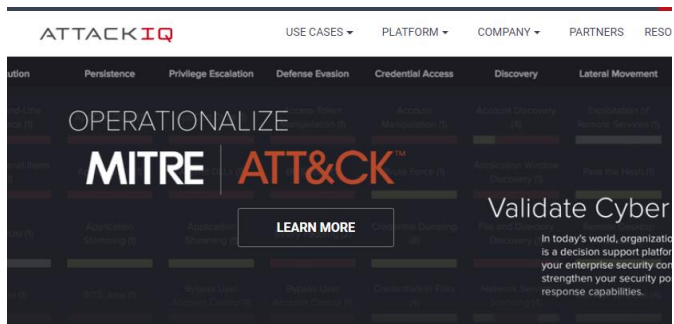
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Share Discovery	Password Policy Discovery	Data from Removable Media	Data Obfuscation	Firmware Corruption	Endpoint Denial of Service
	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	Pass the Hash		Domain Fronting	Inhibit System Recovery	
		Bootkit		Component Firmware		Peripheral Device Discovery	Pass the Ticket				

<https://mitre-attack.github.io/attack-navigator/enterprise/>

Herramientas que proporcionan mecanismos para probar este tipo de técnicas en entornos controlados y que ya están alineadas con ATT&CK



<https://www.verodin.com/>



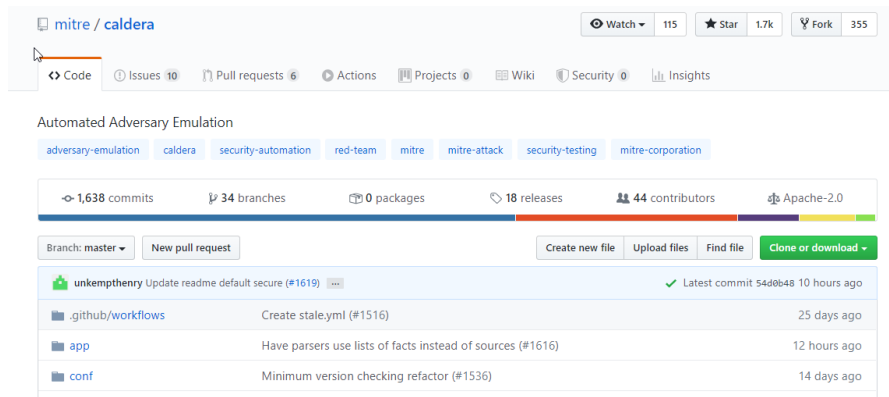
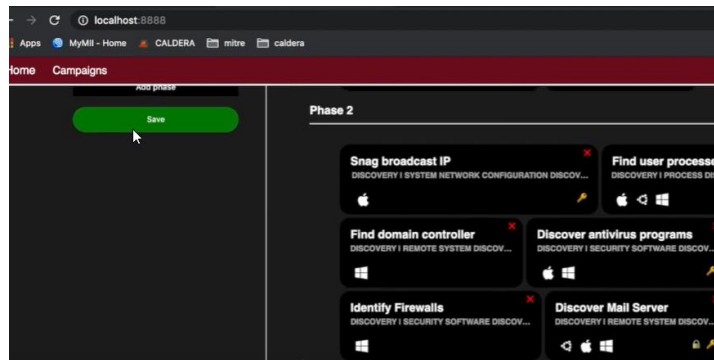
<https://attackiq.com/>



<https://safebreach.com/>

Opciones de código abierto

- <https://github.com/mitre/caldera>
- <https://github.com/uber-common/metta>
- <https://github.com/endgameinc/RTA>
- <https://github.com/redcanaryco/atomic-red-team>



<https://www.youtube.com/watch?v=mVGjqu03fg>

DEMO

<https://mitre-attack.github.io/attack-navigator/enterprise/>

Actividad

- Realice un evaluación de ataque empleando APT32, en el cual el acceso inicial se realiza mediante Spearphishing link.
- Describa cada una de las fases y como el componente identificado en ellas es explotado

Pensamiento Gerencial



RSS (<https://www.incibe-cert.es/feed/vulnerabilities>)

Boletines (<https://www.incibe-cert.es/suscripciones>).

Grupos temáticos: Telegram -- Facebook.

Foros.

Base de Datos.

Revistas Especializadas.

Organismos de estandarización.

Fuentes

- <https://www.welivesecurity.com/la-es/2015/06/25/cvss-version-3/>
<https://www.redhat.com/es/topics/security/what-is-cve>
<https://cve.mitre.org/>
<https://www.redhat.com/en/topics/security/what-is-cve>
<https://nvd.nist.gov/info>
<https://github.com/mitre/caldera>
<https://github.com/uber-common/metta>
<https://github.com/endgameinc/RTA>
<https://github.com/redcanaryco/atomic-red-team>



Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

Muchas gracias ¿Preguntas?



esdeguecol



@esdegue



Escuela Superior
de Guerra



Escuela Superior
de Guerra



esdeguecol



esdeguecol



esdeguecol



issuu
esdeguecol

