Università degli Studi di Salerno

Dipartimento di Informatica

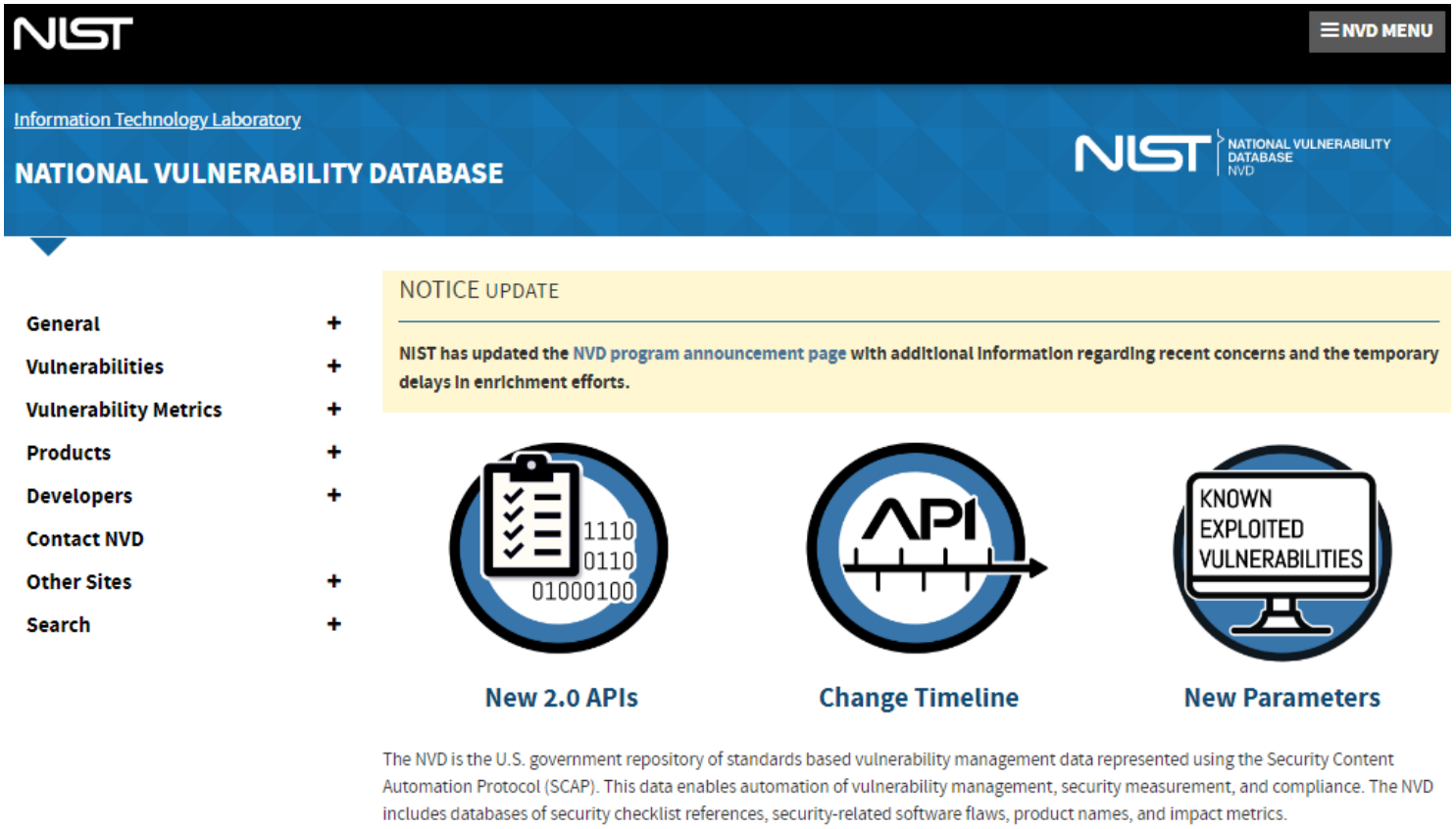
Penetration Testing & Ethical Hacking

Vulnerability Mapping
Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Caratterizzazione delle Vulnerabilità
National Vulnerability Database (NVD)

- **`https://nvd.nist.gov/`**



Caratterizzazione delle Vulnerabilità
National Vulnerability Database (NVD)

- Il **N**ational **V**ulnerability **D**atabase (**NVD**) è un archivio di informazioni **CVE** gestito dal **N**ational **I**nstitute of **S**tandards and **T**echnology (**NIST**)
  - **CVE** (**C**ommon **V**ulnerabilities and **E**xposures)
  - Maggiori dettagli successivamente…

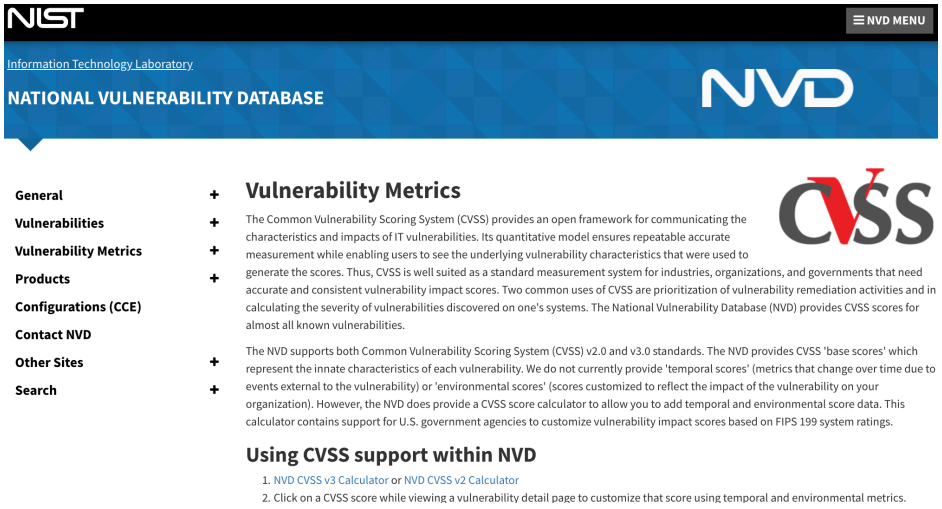
- Costituisce una fonte molto completa di informazioni sulle vulnerabilità

Caratterizzazione delle Vulnerabilità
National Vulnerability Database (NVD)

- I punti chiave del **N**ational **V**ulnerability **D**atabase (**NVD**) sono
  - **Aggregazione**: il NVD aggrega le informazioni sui CVE, inclusi dettagli sulla gravità (*Severity*) delle vulnerabilità, risposte dei fornitori e patch disponibili
    - **Risorsa centralizzata** per accedere alle **informazioni sulle vulnerabilità**
  - **Severity Scoring**: il NVD assegna punteggi CVSS ai CVE, aiutando le organizzazioni a valutare la gravità e l'impatto delle vulnerabilità
  - **Riferimenti**: il NVD include riferimenti a risorse esterne, come avvisi di sicurezza, exploit e patch
    - Risorsa imprescindibile per chi desidera risolvere o mitigare le proprie vulnerabilità

Caratterizzazione delle Vulnerabilità
CVSS e National Vulnerability Database (NVD)

- Il **CVSS** rappresenta un elemento chiave per il **N**ational **V**ulnerability **D**atabase (**NVD**) e per tutte le tassonomie delle vulnerabilità
  - Maggiori dettagli in seguito…



https://nvd.nist.gov/vuln-metrics/cvss

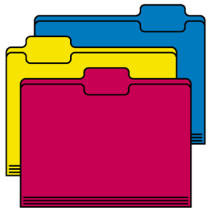
Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- **Tassonomia delle Vulnerabilità**
- Analisi Manuale delle Vulnerabilità
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Tassonomia delle Vulnerabilità

- Con l'aumentare del numero delle tecnologie sono state introdotte varie tassonomie per categorizzare tutte le vulnerabilità note

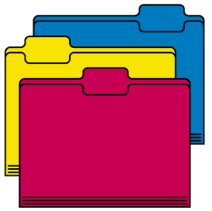
- **Tuttavia**
  - Nessuna tassonomia contiene una lista esaustiva di tutte le vulnerabilità che possono impattare sulla sicurezza di un asset
  - Una singola vulnerabilità potrebbe rientrare in più tassonomie



Tassonomia delle Vulnerabilità

- Le tassonomie aiutano a identificare la maggior parte dei problemi di sicurezza (*vulnerabilità*) noti
  - Tranne le vulnerabilità sconosciute (note come *0-day*)

- La maggior parte di queste tassonomie è già utilizzata dagli strumenti automatici per la valutazione della sicurezza
  - Maggiori dettagli il seguito…



Tassonomia delle Vulnerabilità

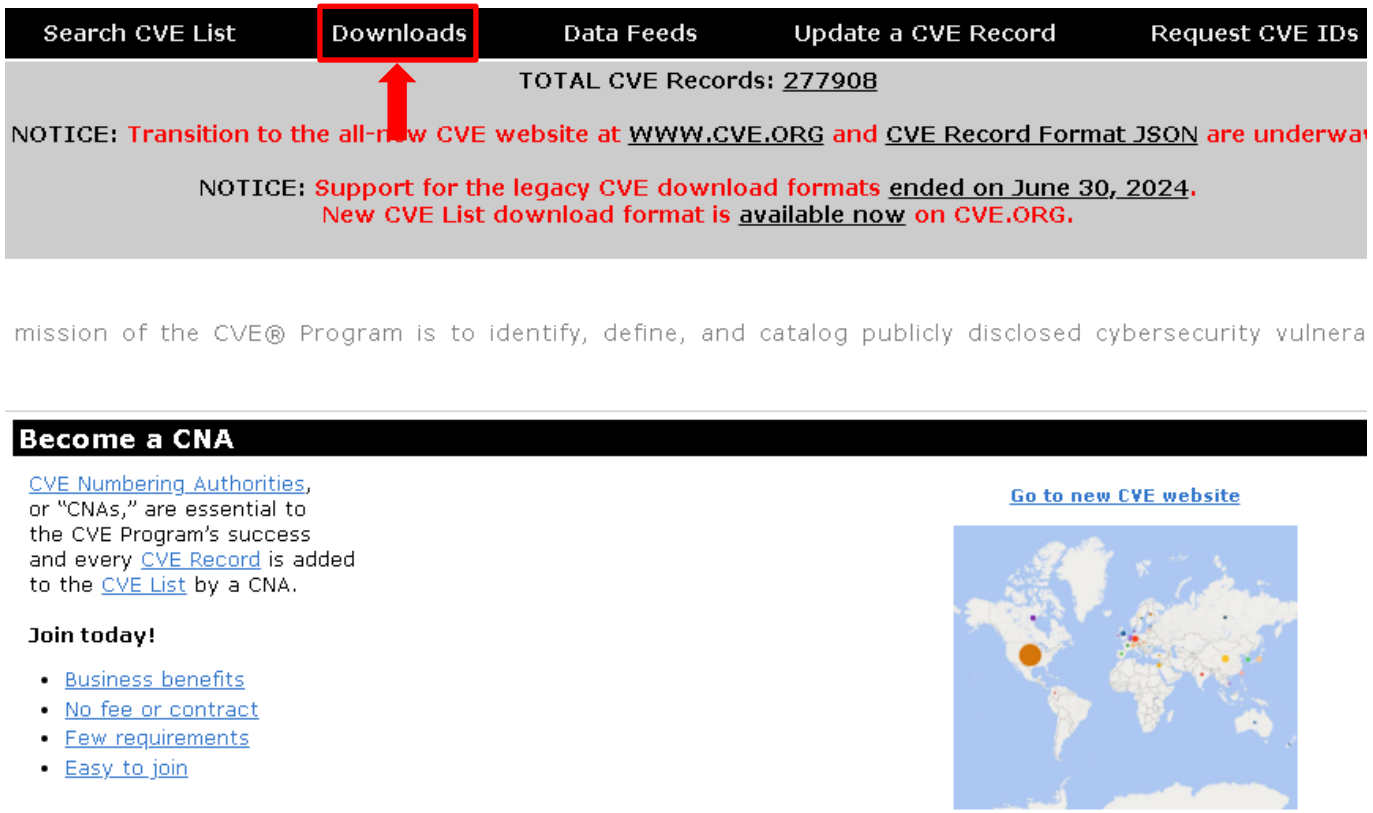
Common Vulnerabilities and Exposure (CVE)

- La tassonomia più comunemente utilizzata per caratterizzare le vulnerabilità è il
  - **CVE** - **C**ommon **V**ulnerabilities and **E**xposure
- Il **CVE** (**C**ommon **V**ulnerabilities and **E**xposures) permette di identificare in maniera univoca e caratterizzare, in maniera «standardizzata» ed universalmente riconosciuta, le **vulnerabilità note**, nei prodotti software e hardware
  - **N.B.** Quindi non contempla vulnerabilità di tipo 0-day
- Tipicamente, quando una vulnerabilità viene scoperta, ad essa viene assegnato un CVE univoco, che la caratterizza e permette la sua diffusione

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

- **https://cve.mitre.org/**



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

- **`https://www.cve.org/Downloads`**

Format	ZIP
CVE JSON	main.zip

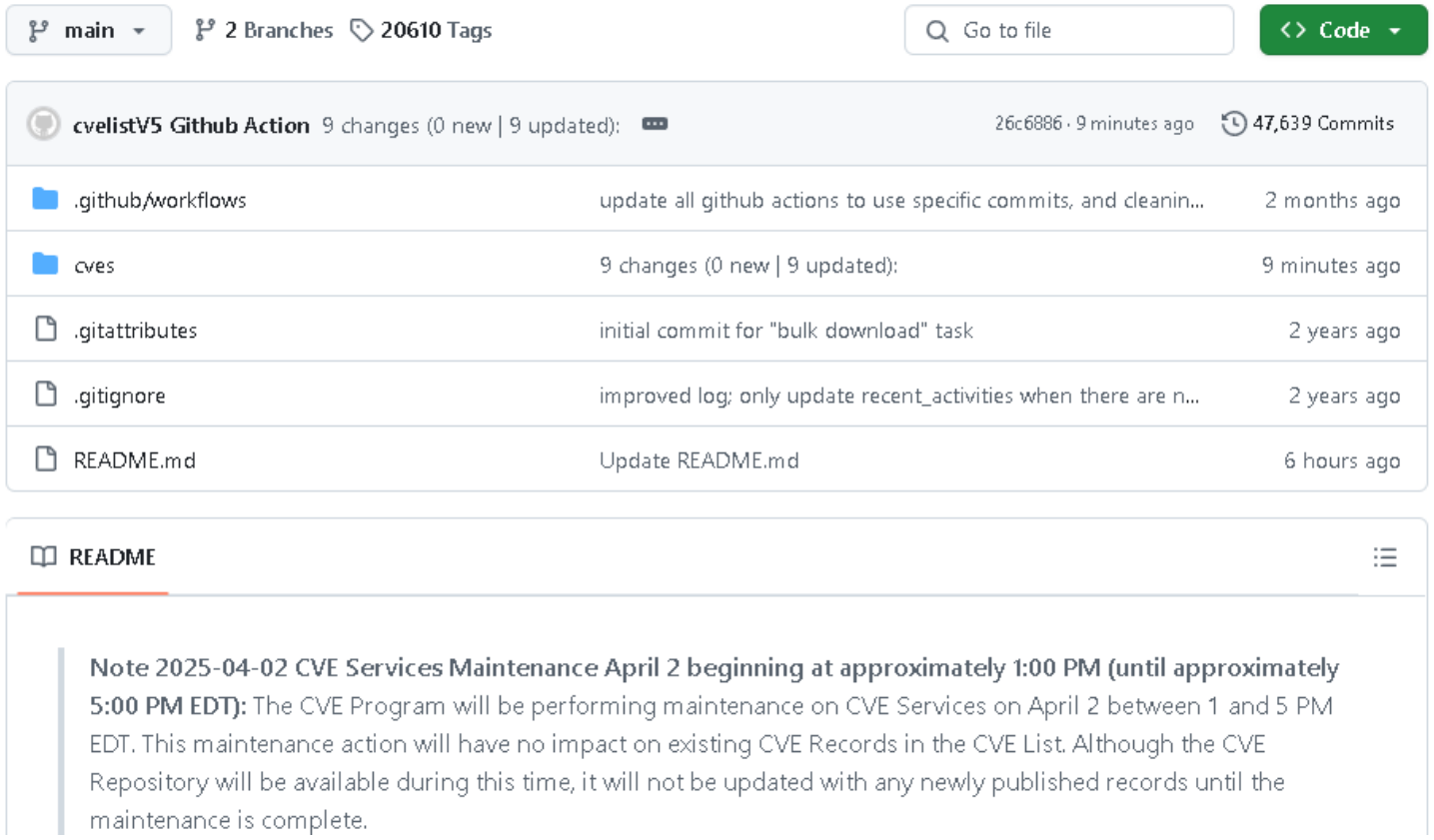
Legacy Format

⚠ **All support for the legacy CVE content download formats (i.e., CSV, HTML, XML, and CVRF) ended on June 30, 2024.** Click **here** for details.

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

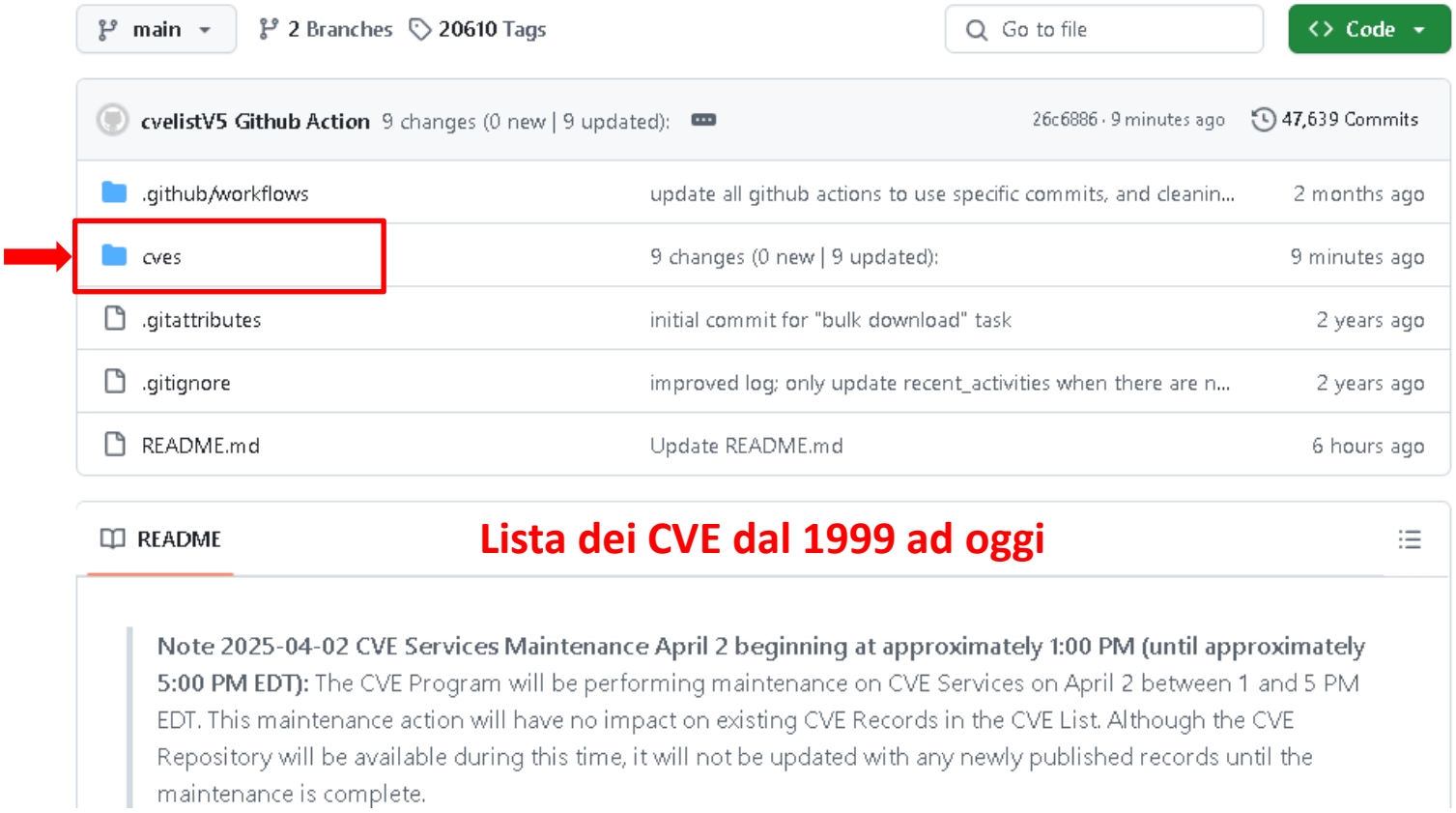
- **https://github.com/CVEProject/cvelistV5**



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

- **https://github.com/CVEProject/cvelistV5**



Tassonomia delle Vulnerabilità

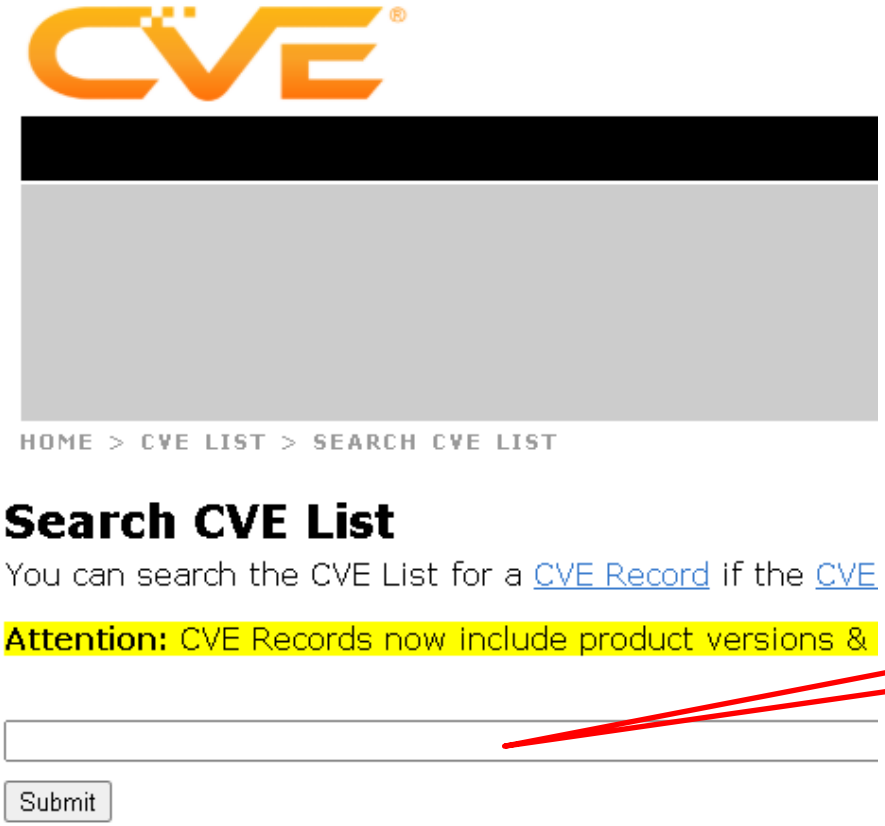
Common Vulnerabilities and Exposure (CVE)

- **https://cve.mitre.org/**

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

- https://cve.mitre.org/cve/search_cve_list.html



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

Search Results

There are **3** CVE entries that match your search.

Name	
CVE-2018-6559	The Linux kernel, as used in Ubuntu 18.04 LTS and Ubuntu 18.10, allows local users to ob a user namespace.
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink
CVE-2018-18653	The Linux kernel, as used in Ubuntu 18.10 and when booted with UEFI Secure Boot enable code by loading arbitrary kernel modules. This occurs because a modified kernel/module.c verification.

SEARCH CVE USING KEYWORD
You can also search by reference u
For More Informatio

Tassonomie CVE relative ad `Ubuntu 18.10`

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

Search Results

There are **3** CVE entries that match your search.

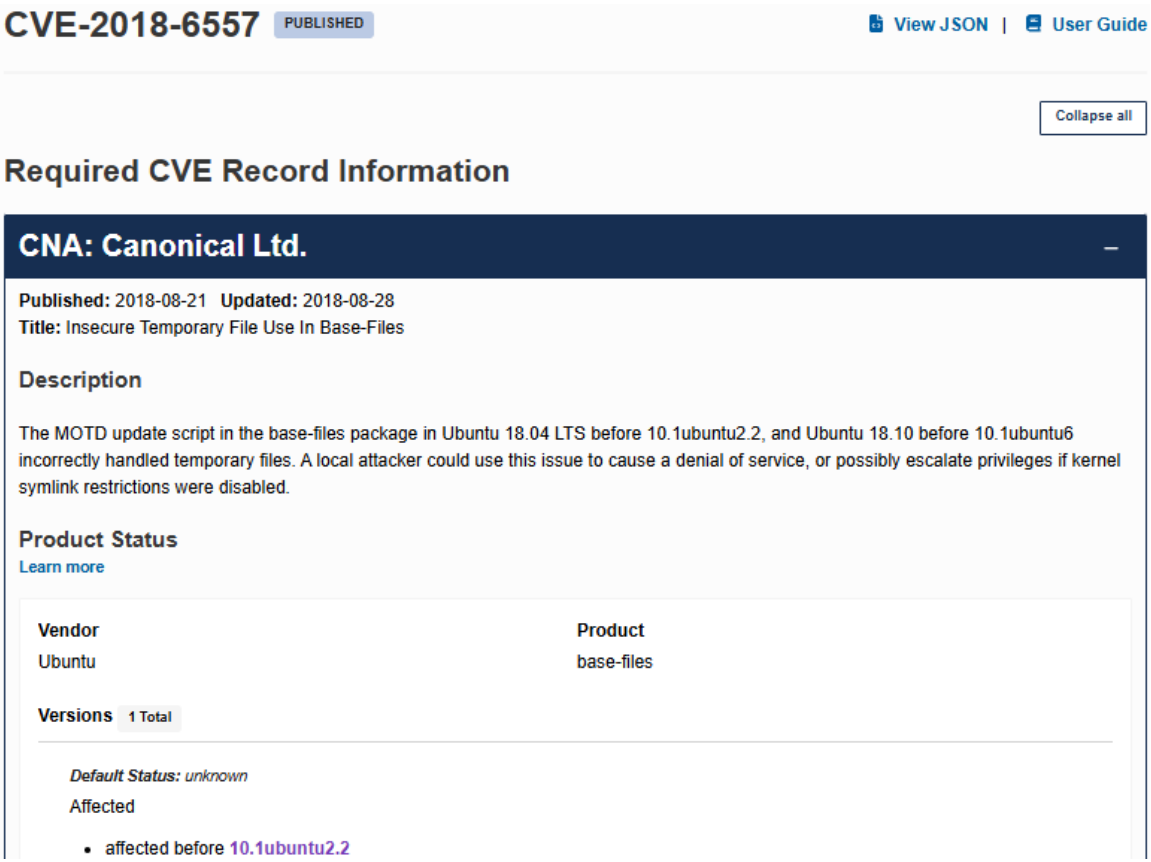
Name	
CVE-2018-6559	The Linux kernel, as used in Ubuntu 18.04 LTS and Ubuntu 18.10, allows local users to ob a user namespace.
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink
CVE-2018-18653	The Linux kernel, as used in Ubuntu 18.10 and when booted with UEFI Secure Boot enable code by loading arbitrary kernel modules. This occurs because a modified kernel/module.c verification.

SEARCH CVE USING KEYWORD
You can also search by reference u
For More Informatio

CVE-2018-6557 (***MOTD*** = ***M****essage* ***O****f* ***T****he* ***D****ay*)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca



CVE-2018-6557 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Canonical Ltd.

Published: 2018-08-21 **Updated:** 2018-08-28
Title: Insecure Temporary File Use In Base-Files

Description

The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled.

Product Status
Learn more

Vendor	Product
Ubuntu	base-files

Versions 1 Total

Default Status: *unknown*
Affected

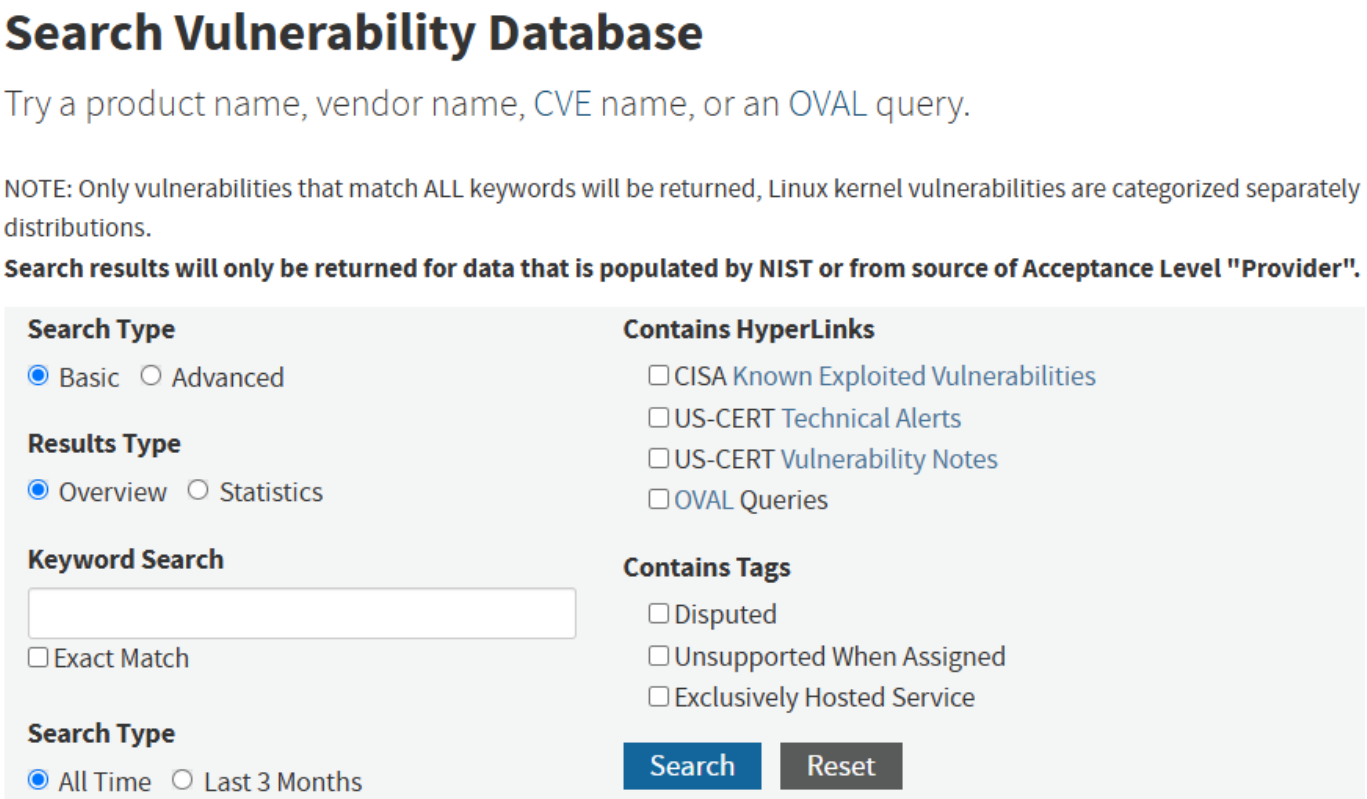
- affected before 10.1ubuntu2.2

Informazioni relative al `CVE-2018-6557`

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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

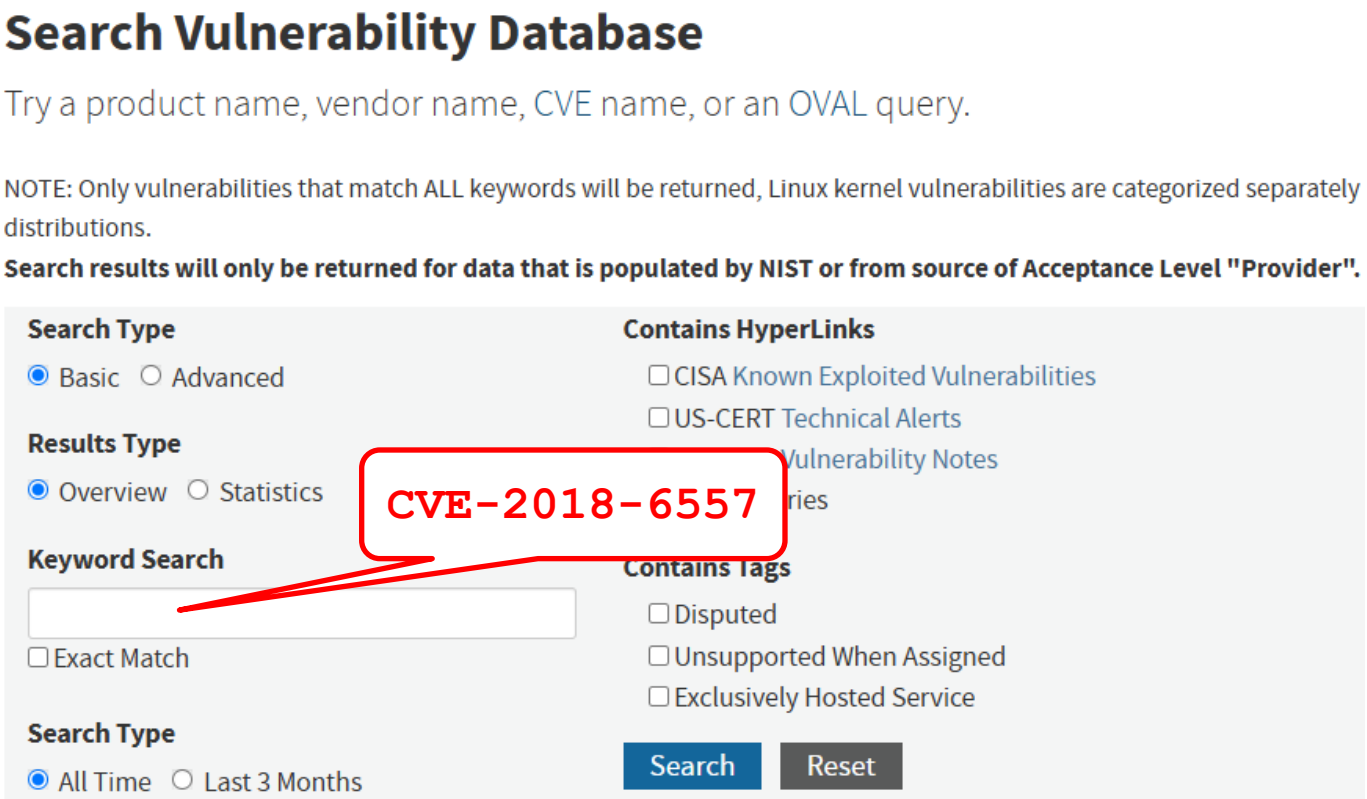


Ricerca di dettagli relativi al `CVE-2018-6557` sul National Vulnerability Database (NVD)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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



Ricerca di dettagli relativi al `CVE-2018-6557` sul National Vulnerability Database (NVD)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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

Vuln ID	Summary	CVSS Severity
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled. **Published:** agosto 21, 2018; 12:29:00 PM -0400	*V4.0:*(not available) *V3.1:* 7.0 HIGH *V2.0:* 4.4 MEDIUM

Ricerca di dettagli relativi al `CVE-2018-6557` sul National Vulnerability Database (NVD)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

CVE-2018-6557 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

QUICK INFO

CVE Dictionary Entry:
CVE-2018-6557
NVD Published Date:
08/21/2018
NVD Last Modified:
11/20/2024
Source:
Canonical Ltd.

Description

The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled.

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.

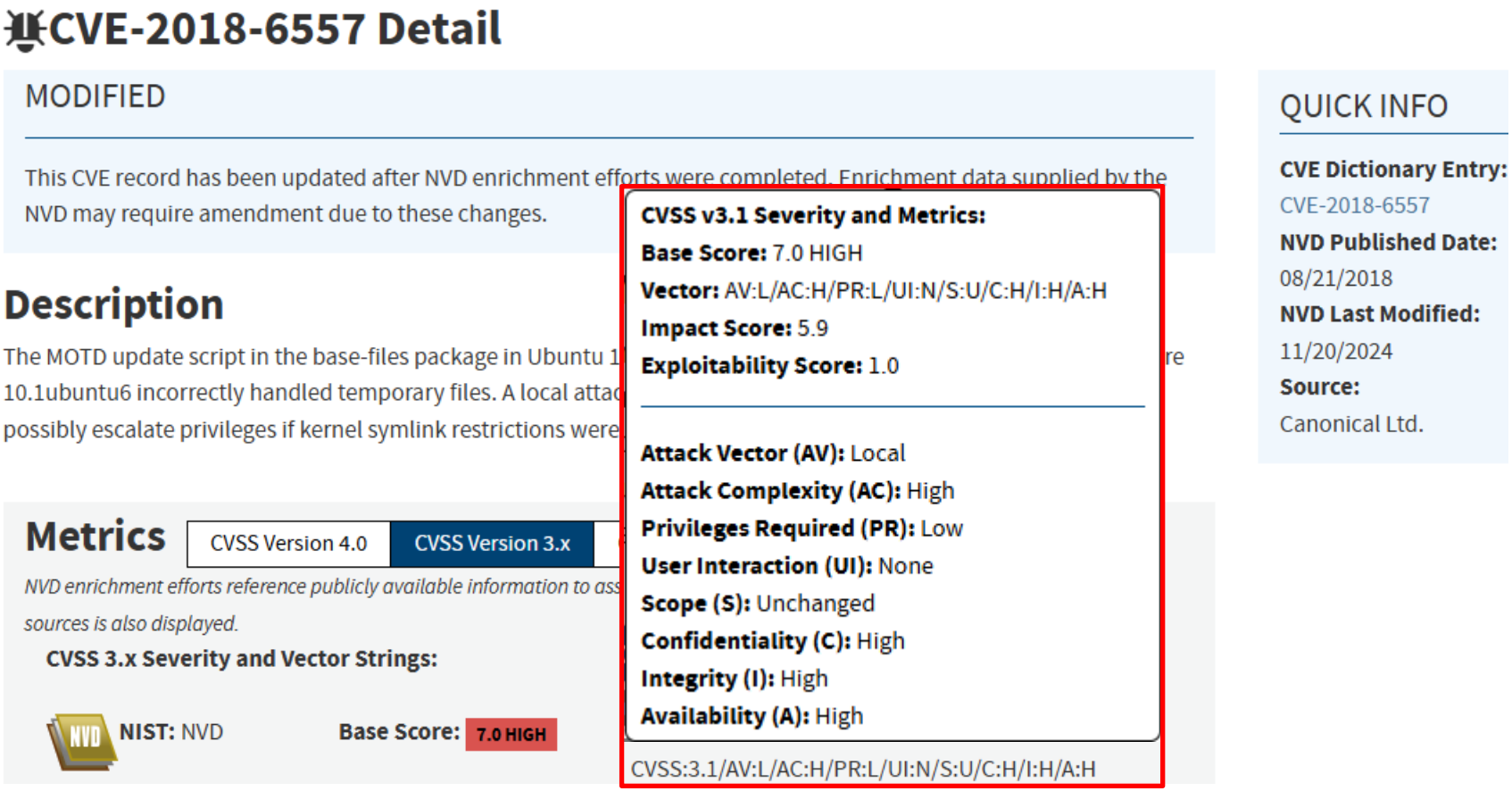
CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 7.0 HIGH **Vector:**
CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Dettagli relativi al `CVE-2018-6557` forniti dal National Vulnerability Database (NVD)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD



Dettagli relativi al `CVE-2018-6557` forniti dal National Vulnerability Database (NVD)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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
http://www.securityfocus.com/bid/105148	Third Party Advisory VDB Entry
http://www.securityfocus.com/bid/105148	Third Party Advisory VDB Entry
http://www.securitytracker.com/id/1041530	Broken Link Third Party Advisory VDB Entry
http://www.securitytracker.com/id/1041530	Broken Link Third Party Advisory VDB Entry
https://usn.ubuntu.com/3748-1/	Vendor Advisory
https://usn.ubuntu.com/3748-1/	Vendor Advisory

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-59	Improper Link Resolution Before File Access ('Link Following')	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:a:base-files_project:base-files:10.1ubuntu2.2:*:*:*:*:*:*:*** Show Matching CPE(s)
- **cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*** Show Matching CPE(s)
- **cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*** Show Matching CPE(s)

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

6 change records found show changes

CWE: Common Weakness Enumeration

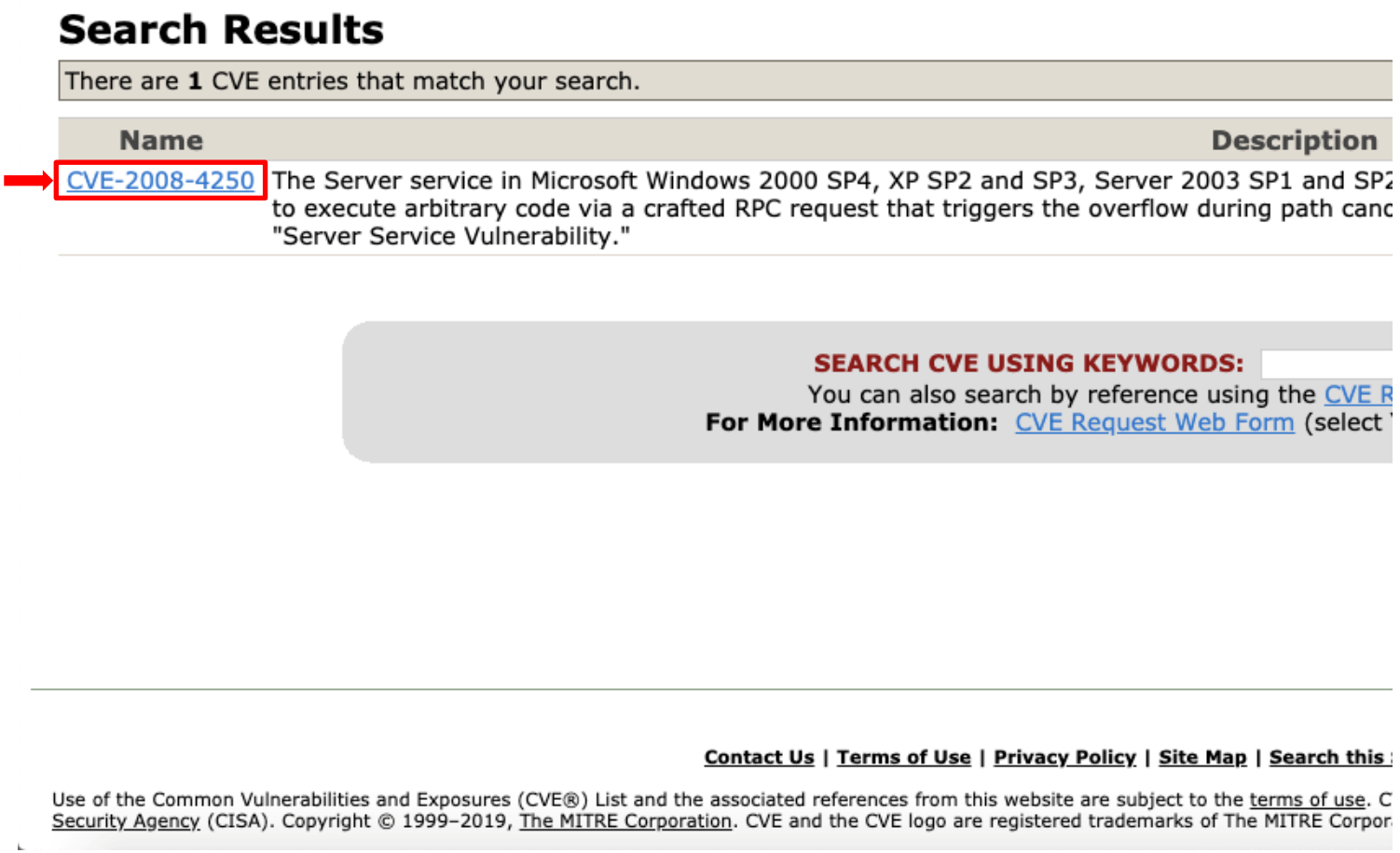
Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

- **MS08-067**
  - Vulnerabilità di Windows XP (e non solo)
  - *MS Server Service Relative Path Stack Corruption*

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca



Search Results

There are **1** CVE entries that match your search.

Name	Description
CVE-2008-4250	The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2 to execute arbitrary code via a crafted RPC request that triggers the overflow during path canc "Server Service Vulnerability."

SEARCH CVE USING KEYWORDS:

You can also search by reference using the CVE R

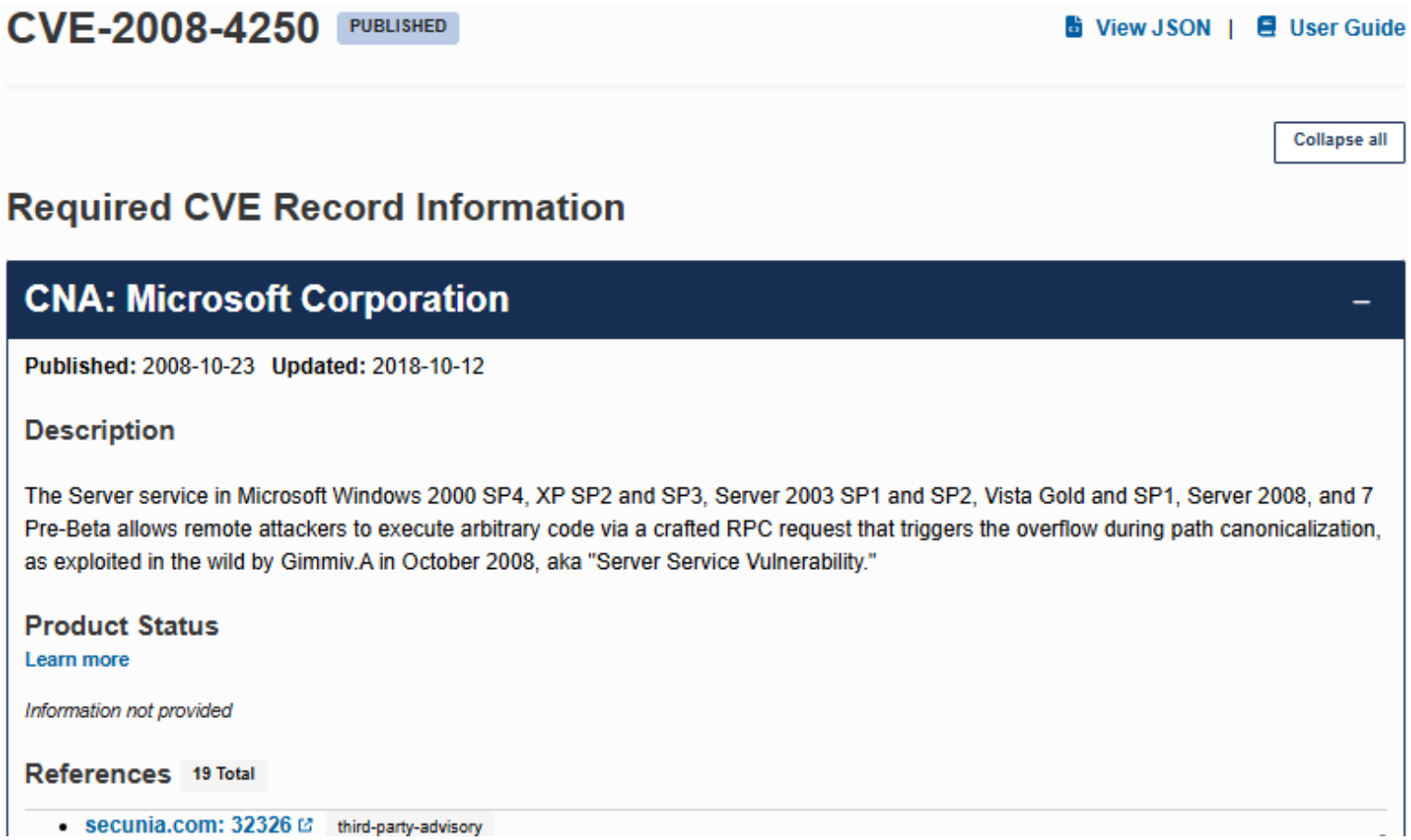
For More Information: CVE Request Web Form (select

Contact Us | Terms of Use | Privacy Policy | Site Map | Search this

Use of the Common Vulnerabilities and Exposures (CVE®) List and the associated references from this website are subject to the terms of use. C
Security Agency (CISA). Copyright © 1999–2019, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corpor

Tassonomia delle Vulnerabilità

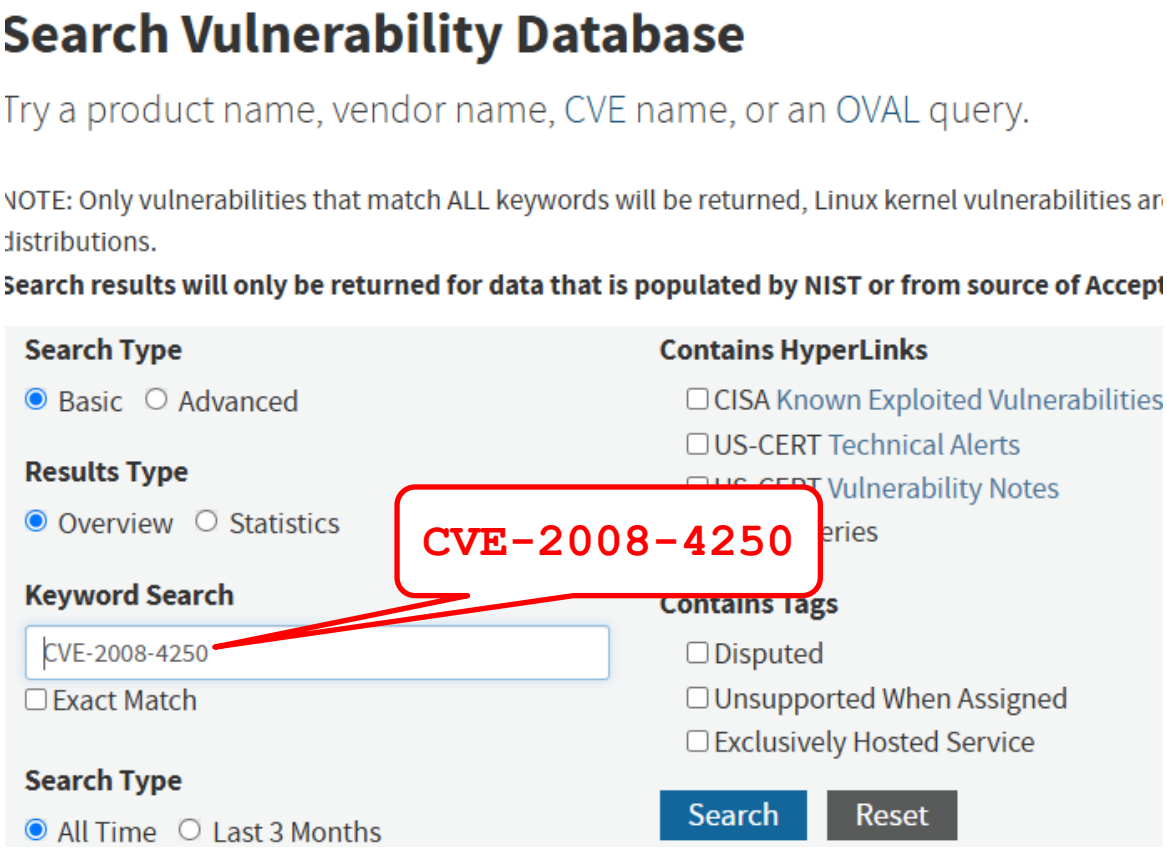
Common Vulnerabilities and Exposure (CVE) – Ricerca



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

CVE-2008-4250

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Published: ottobre 23, 2008; 6:00:01 PM -0400

V4.0:(not available)
V3.x:(not available)
V2.0: **10.0 HIGH**

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

CVE-2008-4250 Detail

DEFERRED

This CVE record is not being prioritized for NVD enrichment efforts due to resource or other concerns.

Description

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

QUICK INFO

CVE Dictionary Entry:
CVE-2008-4250
NVD Published Date:
10/23/2008
NVD Last Modified:
04/08/2025
Source:
Microsoft Corporation

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 2.0 Severity and Vector Strings:

NIST: NVD **Base Score:** 10.0 HIGH **Vector:** (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

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
http://blogs.securiteam.com/index.php/archives/1150	uired
http://blogs.securiteam.com/index.php/archives/1150	uired
https://www.exploit-db.com/exploits/7104	Exploit Third Party Advisory VDB Entry
https://www.exploit-db.com/exploits/7132	Exploit Third Party Advisory VDB Entry
https://www.exploit-db.com/exploits/7132	Exploit

Exploit per sfruttare la vulnerabilità

Tassonomia delle Vulnerabilità

Common Vulnerabilitie… …e (CVE) – NVD

CWE: Common Weakness Enumeration

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-94	Improper Control of Generation of Code ('Code Injection')	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

- **cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:o:microsoft:windows_server_2003:-:*:*:*:*:*:x64:***
  Show Matching CPE(s)
- **cpe:2.3:o:microsoft:windows_server_2003:-:sp1:*:*:*:*:*:*:***
  Show Matching CPE(s)
- **cpe:2.3:o:microsoft:windows_server_2003:-:sp1:*:*:-:*:itanium:***
  Show Matching CPE(s)
- **cpe:2.3:o:microsoft:windows_server_2003:-:sp2:*:*:*:*:*:*:***
  Show Matching CPE(s)

Sistemi operativi affetti dalla vulnerabilità

Tassonomia delle Vulnerabilità

CVE Details

- **https://www.cvedetails.com/**

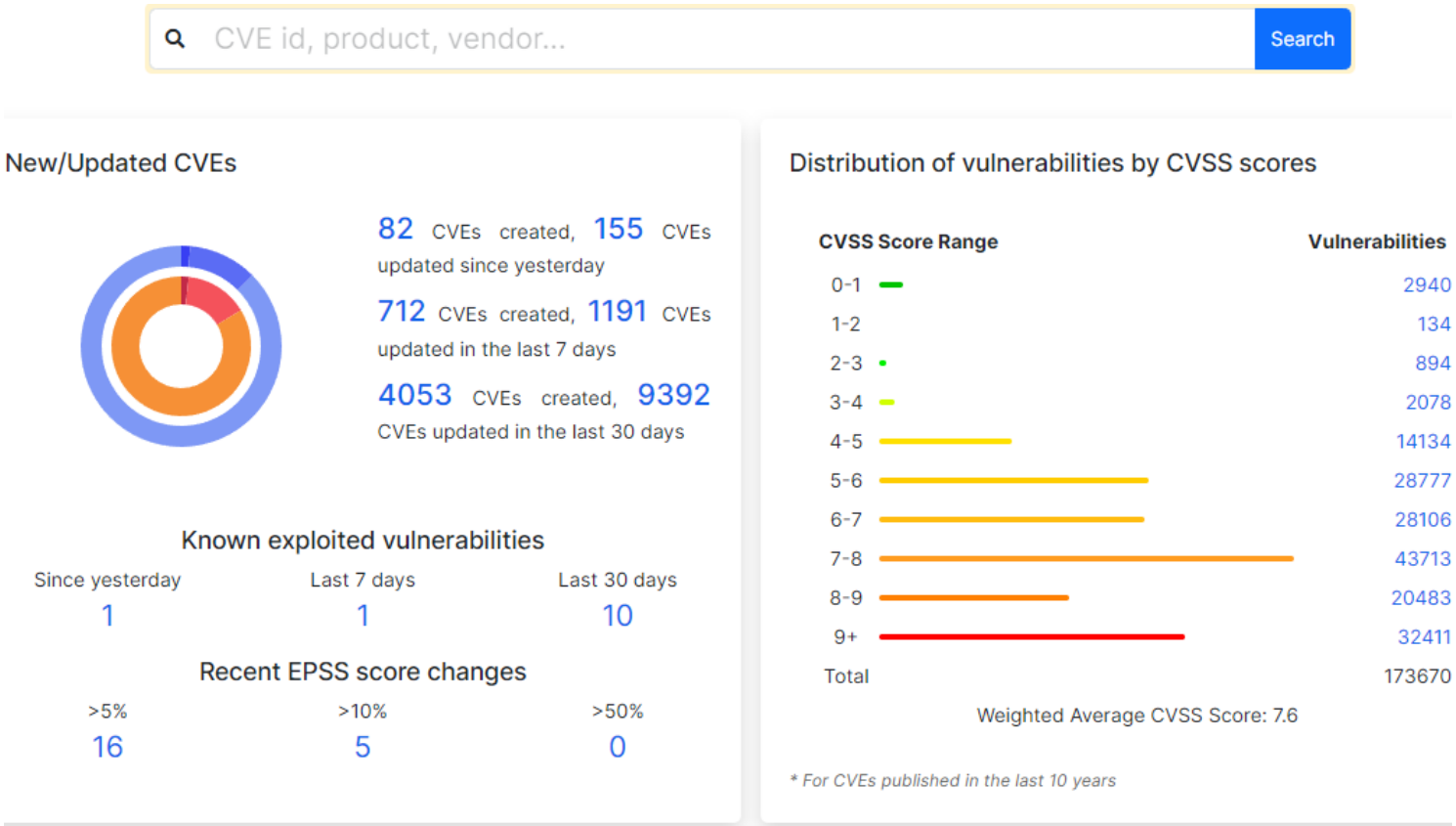
- Fornisce un'interfaccia Web facile da usare verso i dati CVE
- Permette di
  - Cercare **vulnerabilità** relative ad **aziende**, **prodotti**, **versioni di prodotti**, etc
    - Visualizzando le entry CVE correlate ad esse
  - Visualizzare **statistiche** su **aziende produttrici**, **prodotti** e **versioni dei prodotti**, etc
- **Molto utile quando si hanno già a disposizione alcune informazioni sull'asset**

CVE Details
The ultimate security vulnerability datasource

Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (Statistiche)

- **https://www.cvedetails.com/**



Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (Statistiche)

- **https://www.cvedetails.com/browse-by-date.php**

Browse Vulnerabilities By Date

Published: Today Yesterday Last 7 days Last 30 days Updated: Today Yesterday Last 7 days Last 30 days

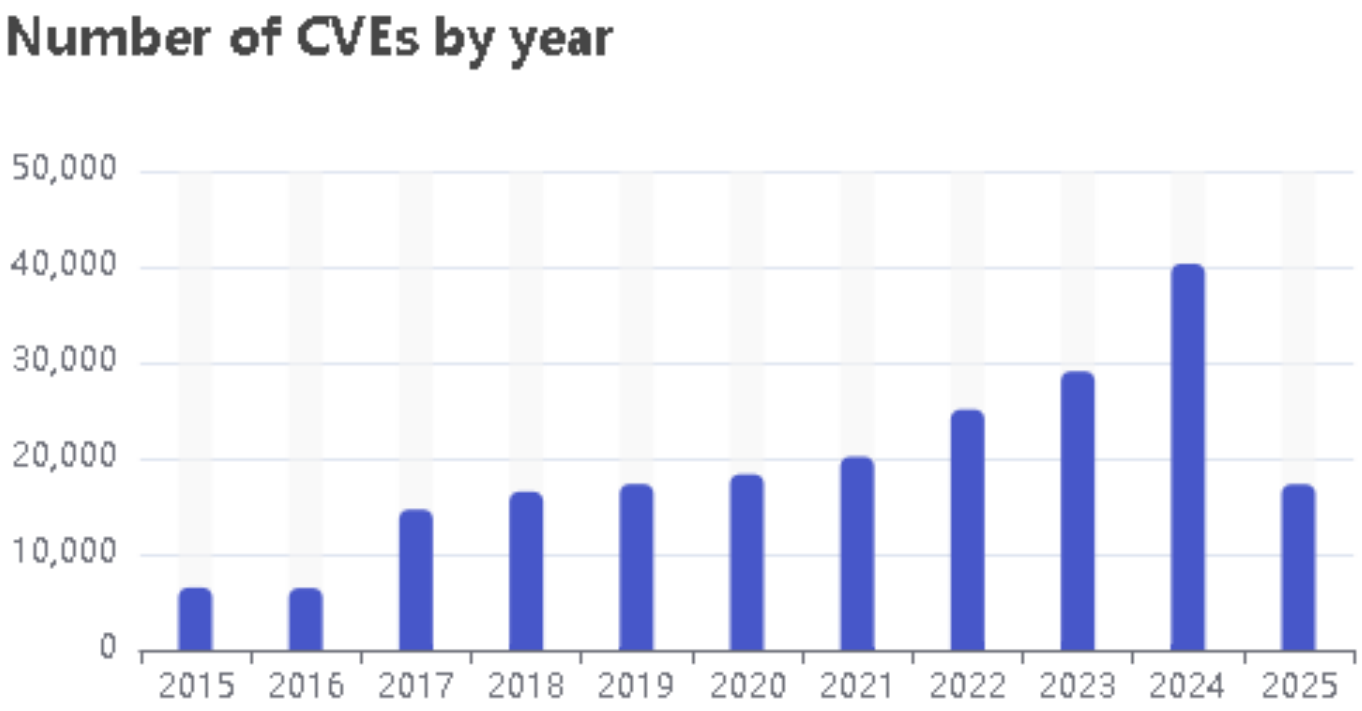
CVEs published in

2025	17285	January	February	March	April	May						
2024	40301	January	February	March	April	May	June	July	August	September	October	November	December
2023	29066	January	February	March	April	May	June	July	August	September	October	November	December
2022	25084	January	February	March	April	May	June	July	August	September	October	November	December
2021	20153	January	February	March	April	May	June	July	August	September	October	November	December
2020	18323	January	February	March	April	May	June	July	August	September	October	November	December
2019	17305	January	February	March	April	May	June	July	August	September	October	November	December
2018	16510	January	February	March	April	May	June	July	August	September	October	November	December
2017	14643	January	February	March	April	May	June	July	August	September	October	November	December
2016	6449	January	February	March	April	May	June	July	August	September	October	November	December
2015	6494	January	February	March	April	May	June	July	August	September	October	November	December

Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (Vulnerabilità per Anno)

- **`https://www.cvedetails.com/browse-by-date.php`**



Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (Vulnerabilità per Tipo)

- **https://www.cvedetails.com/vulnerabilities-by-types.php**

Year	Overflow	Corruption	Sql Injection	XSS	Traversal	Inclusion	CSRF	XXE	SSRF	Redirect	Validation
2015	343	1093	216	773	146	3	248	49	8	46	0
2016	418	1096	85	476	90	4	85	39	15	28	0
2017	2473	1541	505	1500	281	154	334	109	57	97	934
2018	2081	1730	503	2039	569	112	479	188	118	85	1241
2019	1202	2028	544	2387	487	126	560	137	103	121	906
2020	1217	1852	464	2201	436	108	415	119	131	100	812
2021	1662	2526	742	2724	548	91	520	126	192	133	676
2022	1821	3069	1766	3384	695	87	766	123	230	139	691
2023	1634	2130	2116	5103	746	111	1392	124	240	169	536
2024	1774	2517	2650	7456	940	255	1435	111	373	119	122
2025	668	937	1258	3754	338	189	1007	37	207	51	0
Total	15293	20519	10849	31797	5276	1240	7241	1162	1674	1088	5918

Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (Vulnerabilità per Tipo di Impatto)

- **https://www.cvedetails.com/vulnerabilities-by-types.php**

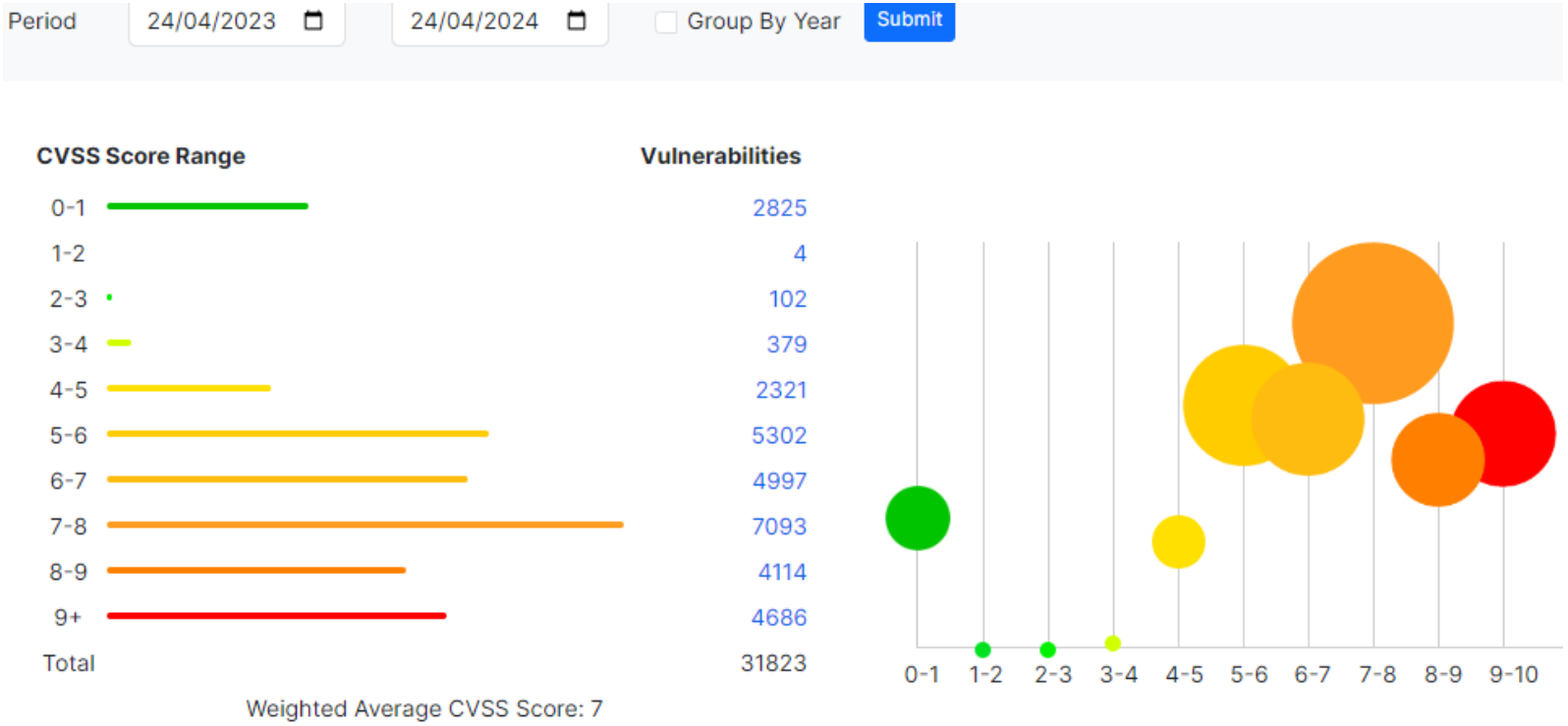
Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2015	1430	0	79	1793	43
2016	1239	1	149	2050	102
2017	1870	845	1014	3372	1384
2018	1728	646	830	2207	1406
2019	1546	663	907	1697	1318
2020	1691	802	1373	1677	1090
2021	2087	779	1091	2297	913
2022	2067	849	1432	2437	1119
2023	2580	878	1345	2560	1433
2024	3971	680	1109	2451	956
2025	974	250	386	953	204
Total	21183	6393	9715	23494	9968

Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (CVSS Score Charts)

- **https://www.cvedetails.com/cvss-score-charts.php**



Tassonomia delle Vulnerabilità

CVE Details – Interfaccia (EPSS Score)

- **https://www.cvedetails.com/epss/epss-score-history.html?delta=110**

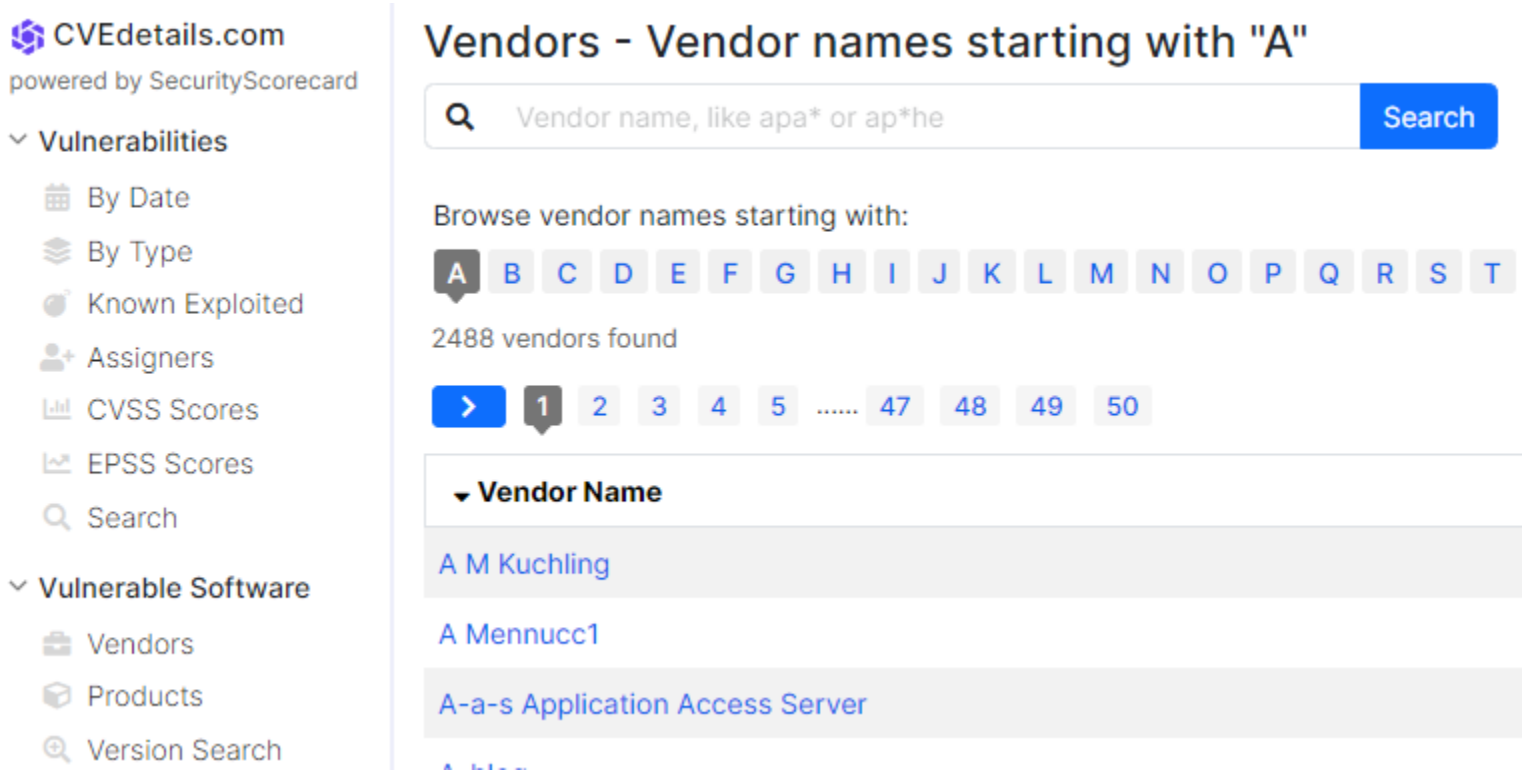
#	Date	CVE	Old EPSS Score	New EPSS Score	Delta (New - Old)
1	2024-04-23	CVE-2014-1774	48.11%	59.76%	+11.65
2	2024-04-23	CVE-2014-1769	48.11%	59.76%	+11.65
3	2024-04-23	CVE-2007-6026	68.92%	81.08%	+12.17
4	2024-04-23	CVE-2007-2644	5.69%	17.36%	+11.67
5	2024-04-23	CVE-2006-2802	9.45%	21.37%	+11.92
6	2024-04-22	CVE-2023-46993	5.36%	70.13%	+64.77
7	2024-04-22	CVE-2023-46979	5.36%	70.13%	+64.77
8	2024-04-22	CVE-2023-46976	5.36%	70.13%	+64.77

Exploit Prediction Scoring System (**EPSS**)

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor

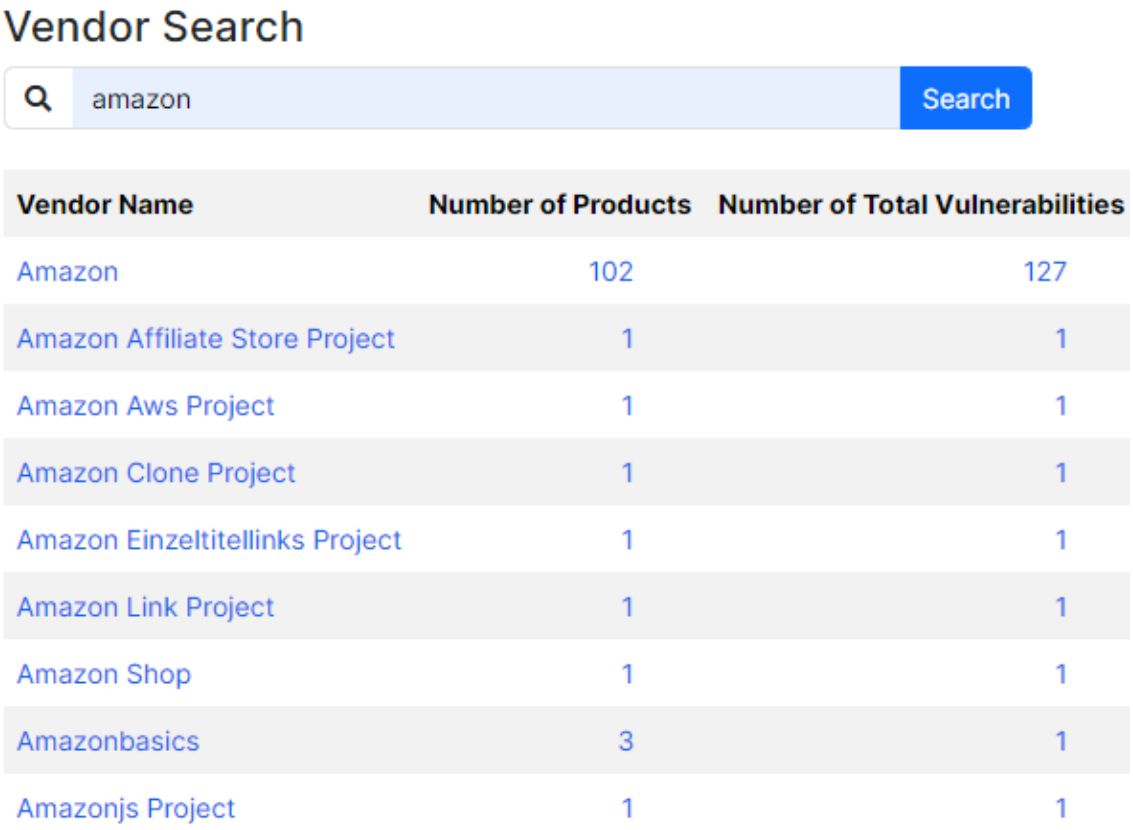
- **`https://www.cvedetails.com/vendor.php`**



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Amazon)

- **`https://www.cvedetails.com/vendor.php`**



Vendor Name	Number of Products	Number of Total Vulnerabilities
Amazon	102	127
Amazon Affiliate Store Project	1	1
Amazon Aws Project	1	1
Amazon Clone Project	1	1
Amazon Einzeltitellinks Project	1	1
Amazon Link Project	1	1
Amazon Shop	1	1
Amazonbasics	3	1
Amazonjs Project	1	1

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Amazon)

- **`https://www.cvedetails.com/vendor.php`**

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	0	0	0	0	0	0	0	0
2017	1	0	0	0	0	2	0	0	0	0	0
2018	2	0	0	5	0	0	0	0	0	0	2
2019	1	1	0	0	0	0	0	0	0	0	0
2020	0	0	0	1	0	0	0	0	0	0	0
2021	6	3	0	0	2	0	0	0	1	0	0
2022	0	0	0	1	1	0	0	0	2	0	0
2023	1	0	0	1	1	0	0	0	0	0	0
2024	0	0	0	1	0	0	0	0	0	0	0
Total	11	4		9	4	2			3		2

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Amazon)

- **`https://www.cvedetails.com/vendor.php`**

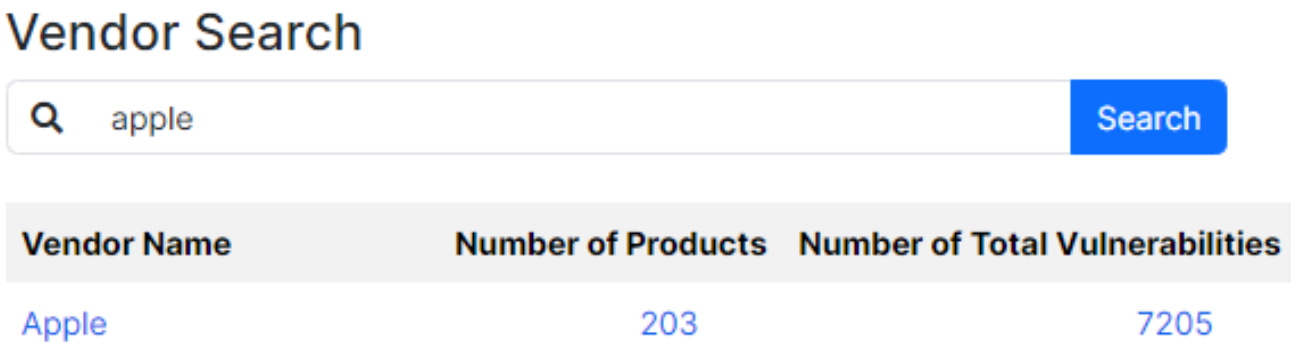
Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	0	0
2017	2	0	0	1	0
2018	5	0	0	1	6
2019	1	0	0	1	0
2020	0	0	0	1	0
2021	4	0	1	2	0
2022	0	0	3	1	4
2023	1	2	2	1	1
2024	0	1	1	1	0
Total	13	3	7	9	11

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Apple)

- **`https://www.cvedetails.com/vendor.php`**



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Apple)

- **`https://www.cvedetails.com/vendor.php`**

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	112	110	1	3	2	0	0	3	0	0	34
2015	297	306	0	3	5	0	1	4	0	0	53
2016	167	180	0	5	0	0	0	1	0	1	22
2017	297	295	0	16	0	1	0	0	0	1	57
2018	69	67	0	2	1	0	0	0	0	1	25
2019	112	233	2	17	1	1	0	0	0	1	76
2020	32	152	0	9	5	0	0	0	0	0	42
2021	37	145	0	7	3	0	0	0	1	2	10
2022	50	139	0	3	0	0	1	1	0	0	8
2023	38	61	0	1	0	1	0	0	0	0	2
2024	3	14	0	0	0	0	0	0	0	0	0
Total	1214	1702	3	66	17	3	2	9	1	6	329

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Apple)

- **`https://www.cvedetails.com/vendor.php`**

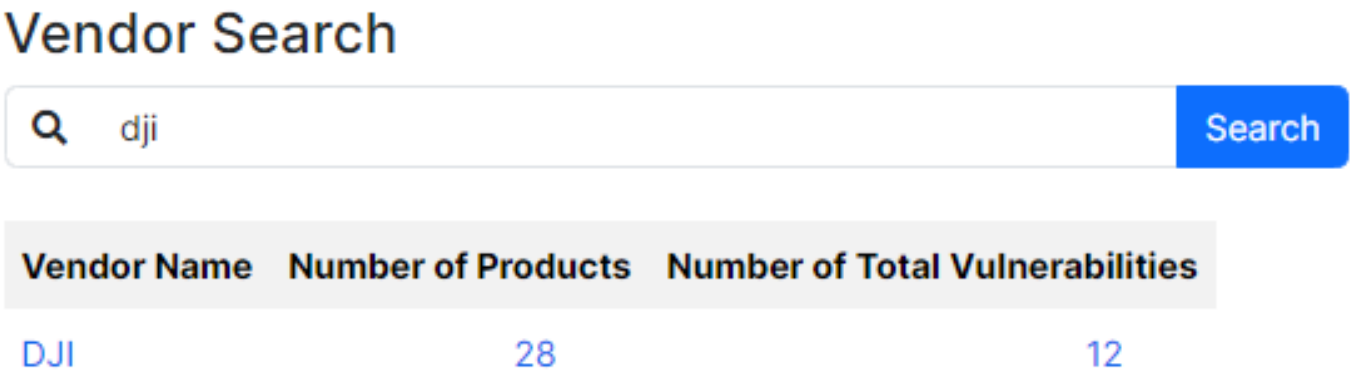
Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	154	4	4	144	22
2015	316	35	35	369	94
2016	157	13	13	215	52
2017	313	4	4	362	81
2018	86	0	1	78	26
2019	37	7	6	19	26
2020	80	0	0	27	13
2021	80	8	8	30	8
2022	98	3	3	20	6
2023	59	3	4	22	2
2024	17	2	1	10	1
Total	1397	79	79	1296	331

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (DJI)

- **`https://www.cvedetails.com/vendor.php`**



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (DJI)

- **https://www.cvedetails.com/vendor.php**

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2021	0	0	0	0	0	0	0	0	0	0	0
2022	0	0	0	0	0	0	0	0	0	0	0
2023	0	0	0	0	0	0	0	0	0	0	0
2024	1	1	0	0	0	0	0	0	0	0	4
Total	1	1									4

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2021	0	0	0	0	0
2022	0	0	0	0	0
2023	0	0	0	0	0
2024	0	0	0	4	0
Total				4	

Tassonomia delle Vulnerabilità

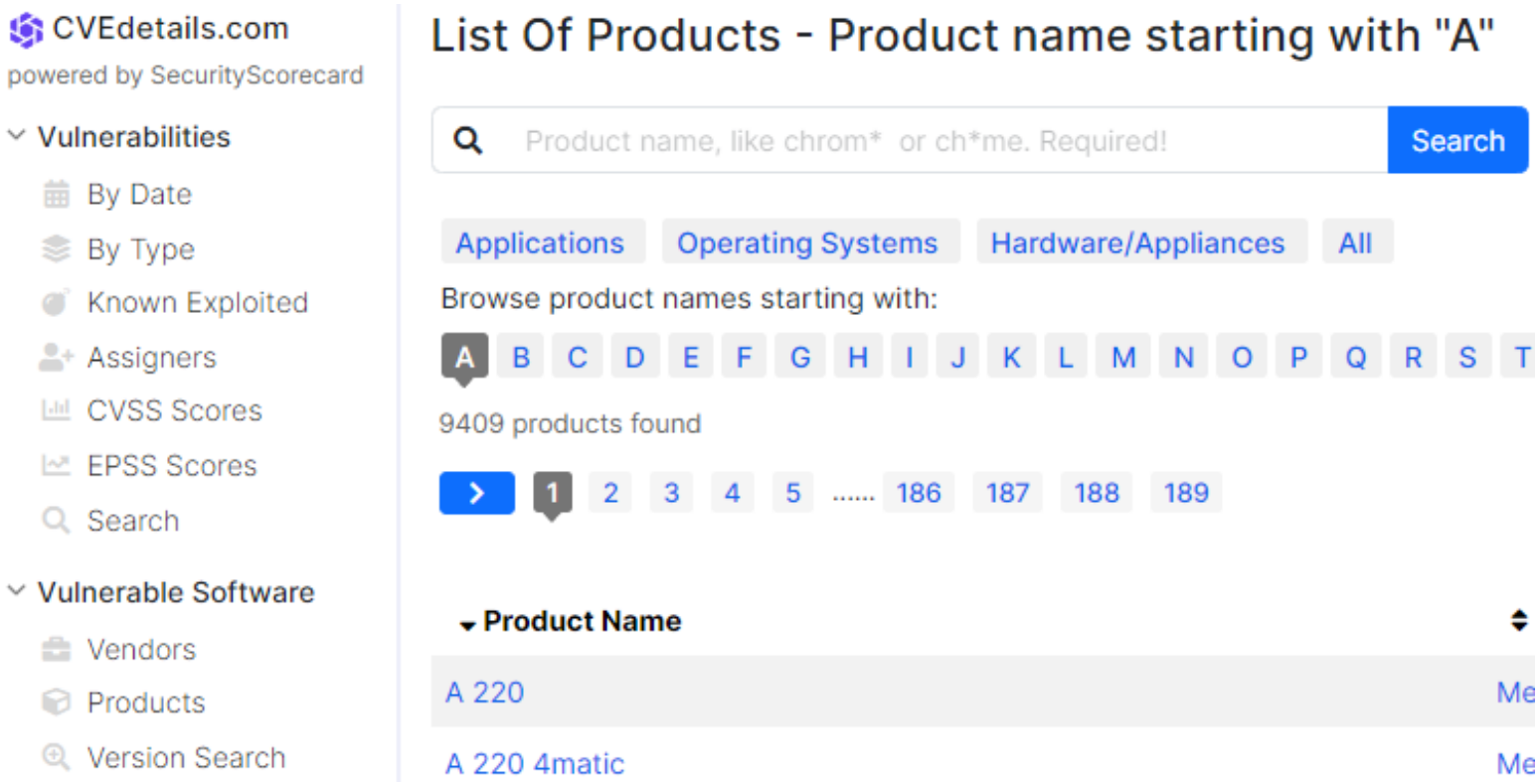
CVE Details – Ricerca per Vendor (Xiaomi)

- **`https://www.cvedetails.com/vendor.php`**

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto

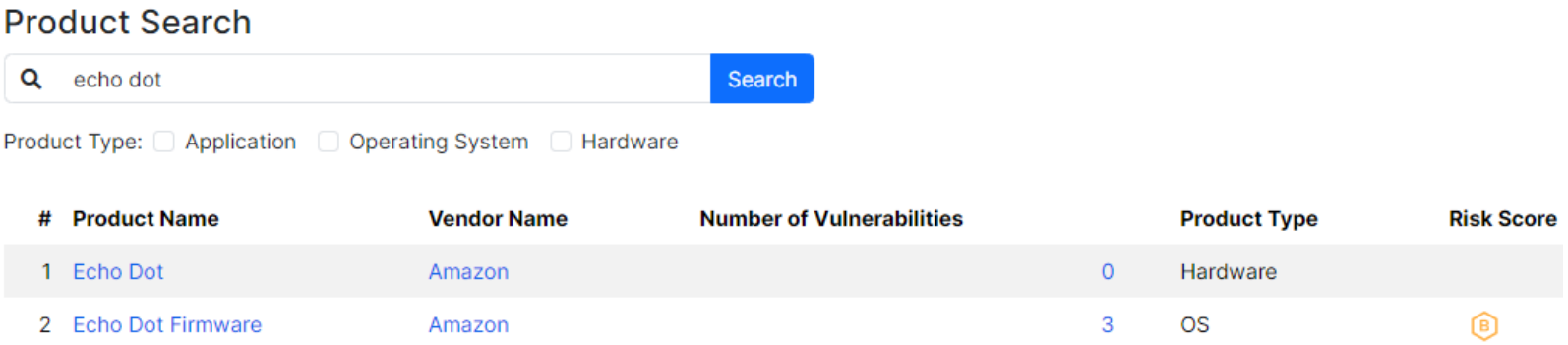
- **`https://www.cvedetails.com/product-list.php`**



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Amazon Echo Dot)

- **`https://www.cvedetails.com/product-list.php`**



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Raspberry)

- **`https://www.cvedetails.com/product-list.php`**

Product Search

raspberry Search

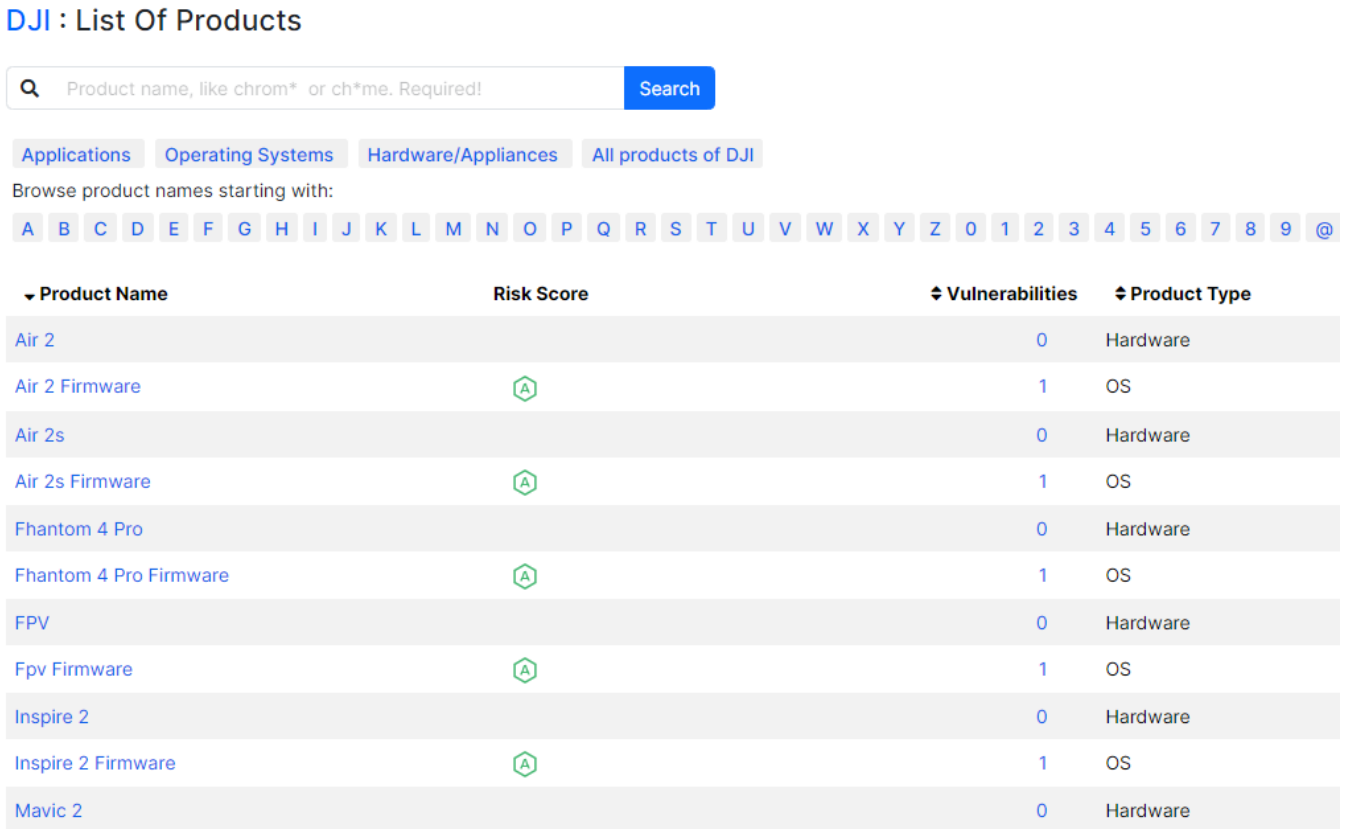
Product Type: Application Operating System Hardware

#	Product Name	Vendor Name	Number of Vulnerabilities	Product Type	Risk Score
1	Raspberry Pi	Codesys	1	Application	
2	Raspberry Pi 3 Model B+	Raspberrypi	0	Hardware	
3	Raspberry Pi 3 Model B+ Firmware	Raspberrypi	2	OS	A
4	Raspberry Pi 4 Model B	Raspberrypi	0	Hardware	
5	Raspberry Pi 4 Model B Firmware	Raspberrypi	1	OS	A
6	Raspberry Pi Os Lite	Raspberrypi	1	OS	B
7	Raspberrymatic	Raspberrymatic	2	OS	B
8	Raspberrytortoise	Raspberrytorte	1	Application	

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Prodotti DJI)

- **`https://www.cvedetails.com/product-list.php`**



DJI : List Of Products

Product name, like chrom* or ch*me. Required! Search

Applications | Operating Systems | Hardware/Appliances | All products of DJI

Browse product names starting with:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9 @

Product Name	Risk Score	Vulnerabilities	Product Type
Air 2		0	Hardware
Air 2 Firmware	A	1	OS
Air 2s		0	Hardware
Air 2s Firmware	A	1	OS
Fhantom 4 Pro		0	Hardware
Fhantom 4 Pro Firmware	A	1	OS
FPV		0	Hardware
Fpv Firmware	A	1	OS
Inspire 2		0	Hardware
Inspire 2 Firmware	A	1	OS
Mavic 2		0	Hardware

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Android)

- **`https://www.cvedetails.com/product-list.php`**

Google » Android (Operating system) : Versions

Versions | Vulnerabilities (**7033**) | Product Dashboard | CVSS Report | Metasploit Modules

This page lists versions of Google » Android which were included in CVE and/or CPE data. Please note that this list is not exhaustive, there may be other versions of this product which we are not aware of.

95 versions found

1 2

Version	Language	Update	Edition	Target Platform	Vulnerabilities	
Android_kernel					0	Version Details
Android_SoC					1	Version Details
2020-06-01					0	Version Details
14					42	Version Details
14.0					95	Version Details
13.1		N/A			97	Version Details

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Android)

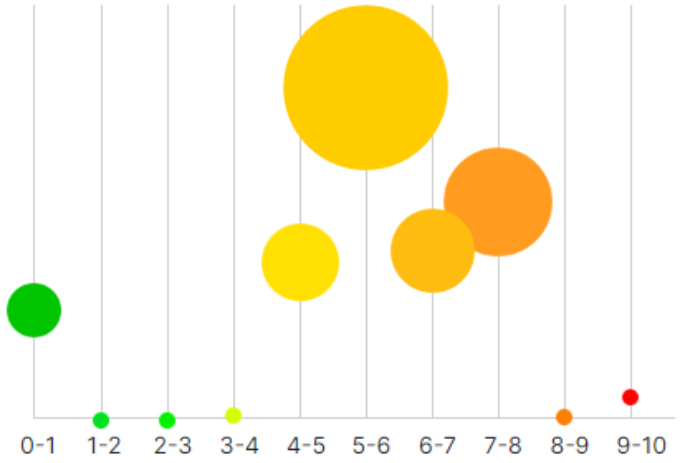
- **`https://www.cvedetails.com/product-list.php`**

Google » Android: CVSS Scores Between 2023-04-24 and 2024-04-24

Period 24/04/2023 24/04/2024 Group By Year Submit

CVSS Score Range	Vulnerabilities
0-1	118
1-2	0
2-3	0
3-4	18
4-5	172
5-6	363
6-7	185
7-8	238
8-9	17
9+	38
Total	1149

Weighted Average CVSS Score: 6.1



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Huawei P40)

- **`https://www.cvedetails.com/product-list.php`**

Product Search

p40 Search

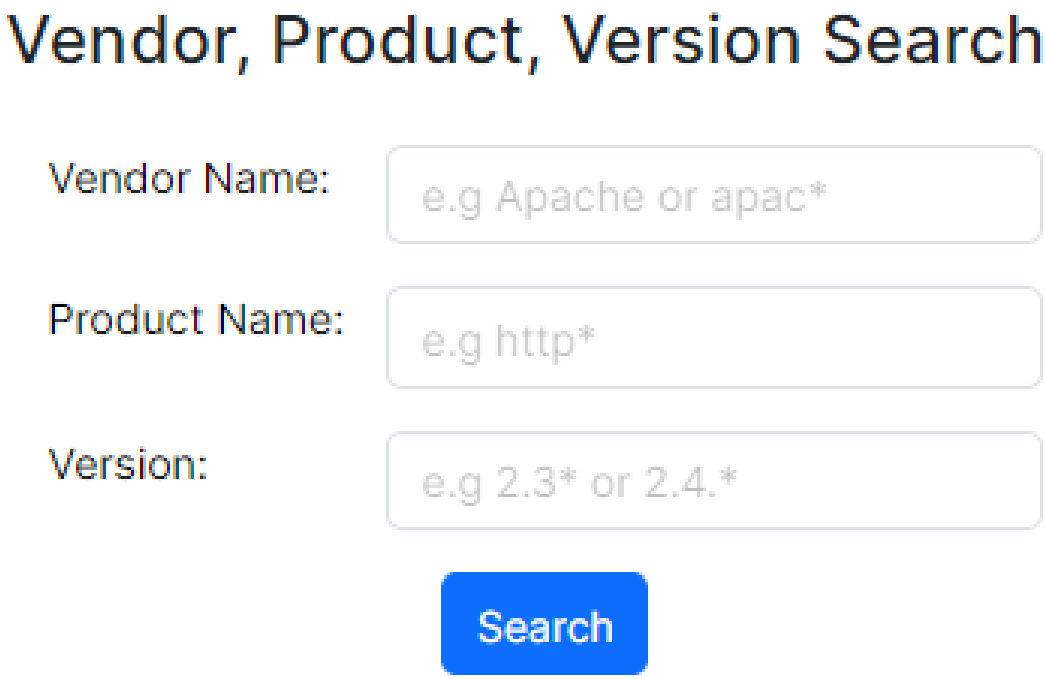
Product Type: Application Operating System Hardware

#	Product Name	Vendor Name	Number of Vulnerabilities	Product Type	Risk Score
1	P40	Huawei	0	Hardware	
2	P40 Firmware	Huawei	2	OS	
3	P40 Pro	Huawei	0	Hardware	
4	P40 Pro Firmware	Huawei	1	OS	

Tassonomia delle Vulnerabilità

CVE Details – Interfaccia

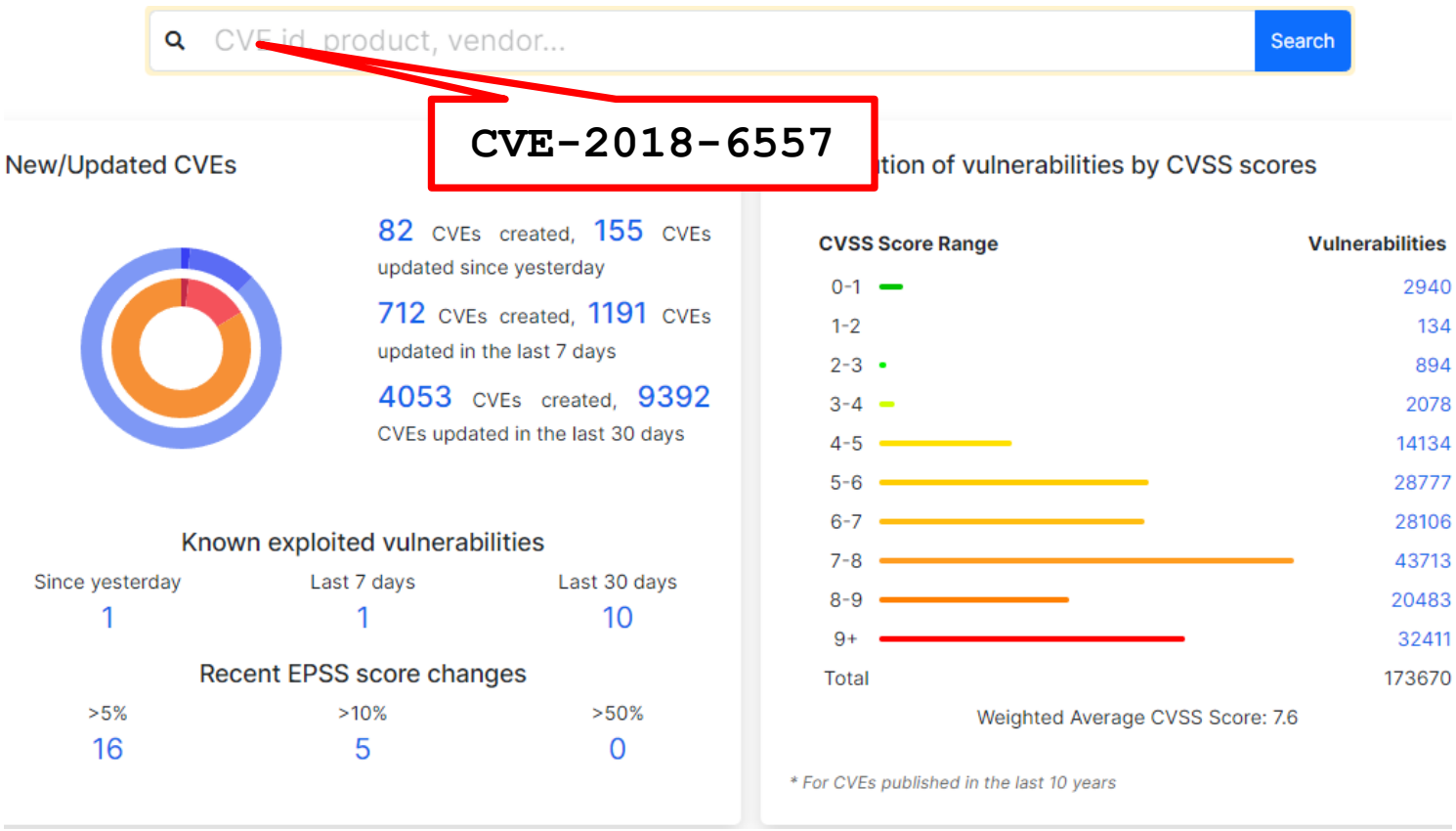
- **`https://www.cvedetails.com/version-search.php`**



Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

- **https://www.cvedetails.com/**



Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

Vulnerability Details : CVE-2018-6557

The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled.

Published 2018-08-21 16:29:01 Updated 2023-01-18 21:22:39 Source Canonical Ltd.

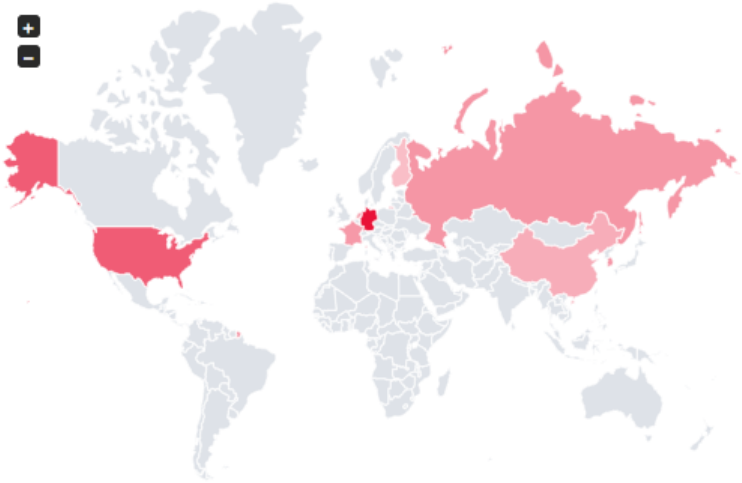
View at NVD, CVE.org

Vulnerability category: Denial of service

Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

Threat overview for CVE-2018-6557



Top countries where our scanners detected CVE-2018-6557

Top open port discovered on systems with this issue **80**

IPs affected by CVE-2018-6557 **6,799**

Threat actors abusing to this issue? **Yes**

Find out if you* are affected by CVE-2018-6557!

*Directly or indirectly through your vendors, service providers and 3rd parties. Powered by attack surface intelligence from SecurityScorecard.

Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

Exploit prediction scoring system (EPSS) score for CVE-2018-6557

Probability of exploitation activity in the next 30 days: 0.04%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 6 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2018-6557

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
4.4	MEDIUM	AV:L/AC:M/Au:N/C:P/I:P/A:P	3.4	6.4	NIST
7.0	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	1.0	5.9	NIST

CWE ids for CVE-2018-6557

CWE-59 Improper Link Resolution Before File Access ('Link Following')

The product attempts to access a file based on the filename, but it does not properly prevent that filename from identifying a link or shortcut that resolves to an unintended resource.

Assigned by: nvd@nist.gov (Primary)

Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

References for CVE-2018-6557

http://www.securitytracker.com/id/1041530

Debian Linux MOTD Update Script Unsafe Temporary File Usage Lets Local Users Deny Service and Gain Elevated Privileges - SecurityTracker

Broken Link;Third Party Advisory;VDB Entry

http://www.securityfocus.com/bid/105148

Debian Linux MOTD Update Script CVE-2018-6557 Insecure Temporary File Handling Vulnerability

Third Party Advisory;VDB Entry

https://usn.ubuntu.com/3748-1/

USN-3748-1: base-files vulnerability | Ubuntu security notices

Vendor Advisory

Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

Products affected by CVE-2018-6557

Canonical » Ubuntu Linux » Version: 18.04 LTS Edition cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*	Matching versions
Canonical » Ubuntu Linux » Version: 18.10 cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*	Matching versions
Base-files Project » Base-files » Version: 10.1ubuntu2.2 cpe:2.3:a:base-files_project:base-files:10.1ubuntu2.2:*:*:*:*:*:*:*	Matching versions

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

- **https://www.cvedetails.com/**

Vulnerabilità MS08-067

CVE-2008-4250 Search

New/Updated CVEs

82 CVEs created, 155 CVEs updated since yesterday

712 CVEs created, 1191 CVEs updated in the last 7 days

4053 CVEs created, 9392 CVEs updated in the last 30 days

Known exploited vulnerabilities

Since yesterday	Last 7 days	Last 30 days
1	1	10

Recent EPSS score changes

>5%	>10%	>50%
16	5	0

Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	2940
1-2	134
2-3	894
3-4	2078
4-5	14134
5-6	28777
6-7	28106
7-8	43713
8-9	20483
9+	32411
Total	173670

Weighted Average CVSS Score: 7.6

** For CVEs published in the last 10 years*

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

Vulnerability Details : CVE-2008-4250 Public exploit exists!

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Published 2008-10-23 22:00:01 Updated 2022-02-09 14:36:44 Source Microsoft Corporation

View at NVD, CVE.org

Vulnerability category: Execute code

Exploit prediction scoring system (EPSS) score for CVE-2008-4250

Probability of exploitation activity in the next 30 days: 97.48%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 100 % EPSS Score History EPSS FAQ

Vulnerabilità MS08-067

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

Metasploit modules for CVE-2008-4250

MS08-067 Microsoft Server Service Relative Path Stack Corruption — Disclosure Date: 2008-10-28 First seen: 2020-04-26

exploit/windows/smb/ms08_067_netapi

This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (alon

More information

CVSS scores for CVE-2008-4250

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score S
10.0	HIGH	AV:N/AC:L/Au:N/C:C/I:C/A:C	10.0	10.0	NIST

Exploit per la vulnerabilità

CWE ids for CVE-2008-4250

CWE-94 Improper Control of Generation of Code ('Code Injection')

The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

Assigned by: nvd@nist.gov (Primary)

Vulnerabilità MS08-067

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

References for CVE-2008-4250

http://www.vupen.com/english/advisories/2008/2902
Vendor Advisory

http://www.securityfocus.com/bid/31874
Exploit;Patch;Third Party Advisory;VDB Entry

http://www.kb.cert.org/vuls/id/827267
Third Party Advisory;US Government Resource

https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6093
Third Party Advisory

https://www.exploit-db.com/exploits/6841
Exploit;Third Party Advisory;VDB Entry

http://marc.info/?l=bugtraq&m=122703006921213&w=2
'[security bulletin] HPSBST02386 SSRT080164 rev.1 - Storage Management Appliance (SMA), Microsoft Pat' - MARC
Issue Tracking;Mailing List;Third Party Advisory

CVEs referencing this url

Vulnerabilità MS08-067

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

Products affected by CVE-2008-4250

Microsoft » Windows 2000 » Version: N/A Update SP4 cpe:2.3:o:microsoft:windows_2000:-:sp4:*:*:*:*:*:*	Matching versions
Microsoft » Windows Xp » Version: N/A Update SP2 cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:*:*:*:*	Matching versions
Microsoft » Windows Xp » Version: N/A Professional Edition For X64 cpe:2.3:o:microsoft:windows_xp:-:-:*:*:professional:*:x64:*	Matching versions
Microsoft » Windows Xp » Version: N/A Update SP3 cpe:2.3:o:microsoft:windows_xp:-:sp3:*:*:*:*:*:*	Matching versions
Microsoft » Windows Xp » Version: N/A Update SP2 Professional Edition For X64 cpe:2.3:o:microsoft:windows_xp:-:sp2:*:*:professional:*:x64:*	Matching versions

Vulnerabilità MS08-067

Tassonomia delle Vulnerabilità

Known Exploited Vulnerabilities (KEV) – Caratteristiche

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Il **K**nown **E**xploited **V**ulnerabilities (**KEV**) è un catalogo, gestito dal U.S. **C**ybersecurity and **I**nfrastructure **S**ecurity **A**gency (**CISA**), che tiene traccia delle vulnerabilità hardware e software in base al loro effettivo sfruttamento
- La CISA detiene quindi una fonte autorevole delle vulnerabilità che sono state sfruttate
- Il catalogo KEV dovrebbe essere utilizzato come parametro in input durante un processo per la prioritizzazione della gestione delle vulnerabilità

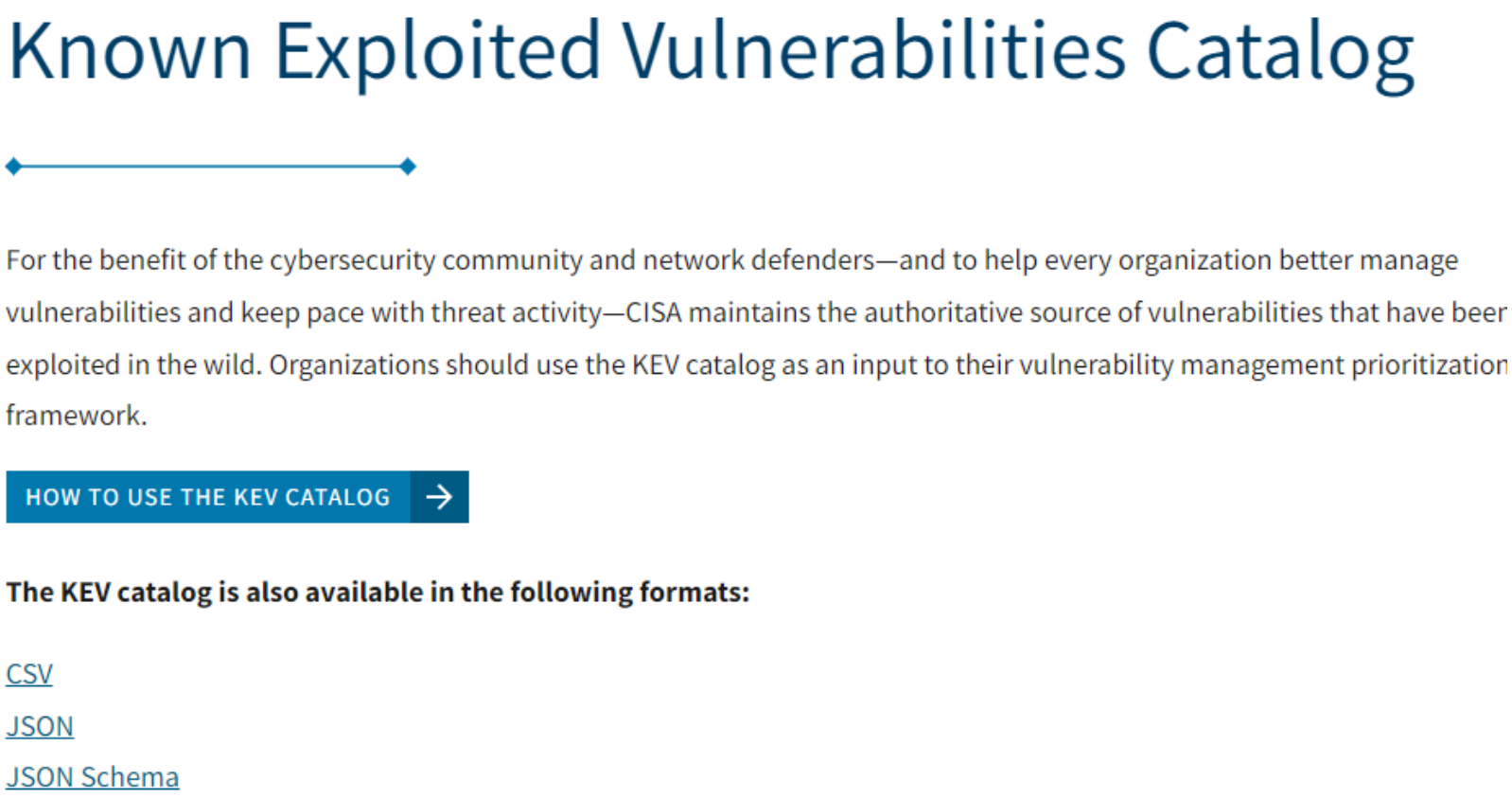
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Tassonomia delle Vulnerabilità

KEV – Interfaccia

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Known Exploited Vulnerabilities Catalog

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have beer exploited in the wild. Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.

HOW TO USE THE KEV CATALOG →

The KEV catalog is also available in the following formats:

CSV

JSON

JSON Schema

Tassonomia delle Vulnerabilità

KEV – Interfaccia

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

MICROSOFT | WINDOWS

CVE-2022-38028

Microsoft Windows Print Spooler Privilege Escalation Vulnerability

Microsoft Windows Print Spooler service contains a privilege escalation vulnerability. An attacker may modify a JavaScript constraints file and execute it with SYSTEM-level permissions.

- **Action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
- **Known To Be Used in Ransomware Campaigns?:** Unknown
- **Date Added:** 2024-04-23
- **Due Date:** 2024-05-14

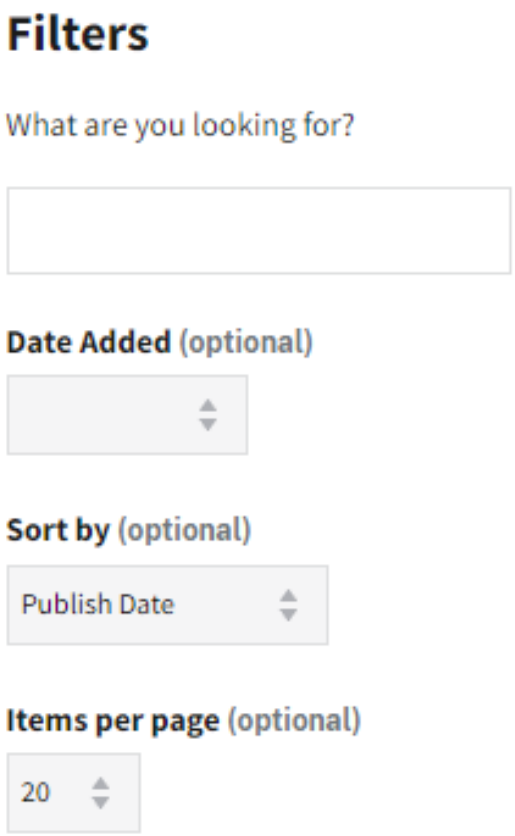
Resources and Notes +

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38028

Tassonomia delle Vulnerabilità

KEV – Ricerca

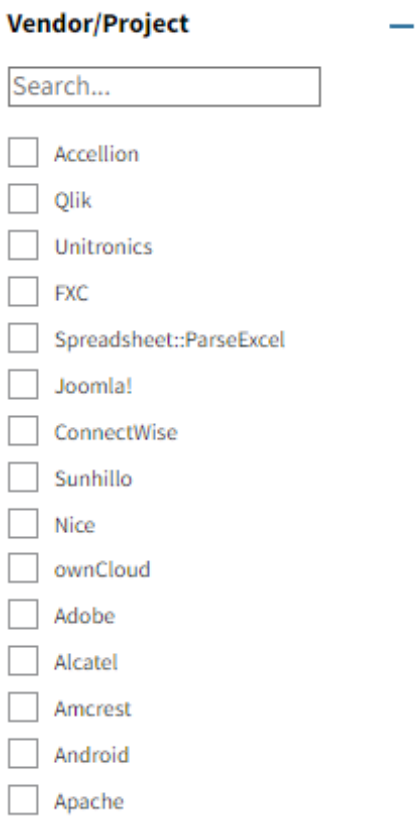
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Tassonomia delle Vulnerabilità

KEV – Ricerca Produttori

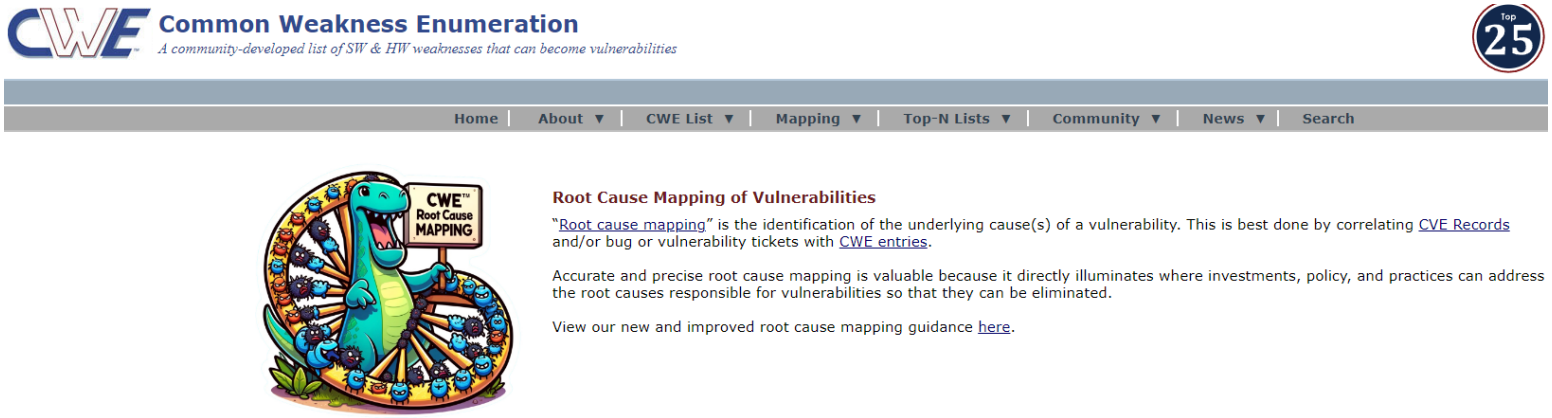
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog



Tassonomia delle Vulnerabilità

Common Weakness Enumeration (CWE)

- **https://cwe.mitre.org/**



- **CVE** è uno standard per identificare in maniera univoca e caratterizzare le vulnerabilità
- **CWE** è uno standard per classificare e descrivere le tipologie di «debolezze» che possono portare a vulnerabilità

Tassonomia delle Vulnerabilità

Common Weakness Enumeration (CWE)

- CWE integra CVE concentrandosi sui tipi di «debolezze» che possono esistere nel software o nell'hardware
- CVE identifica istanze specifiche di vulnerabilità, CWE classifica i difetti o le debolezze comuni che possono portare a vulnerabilità

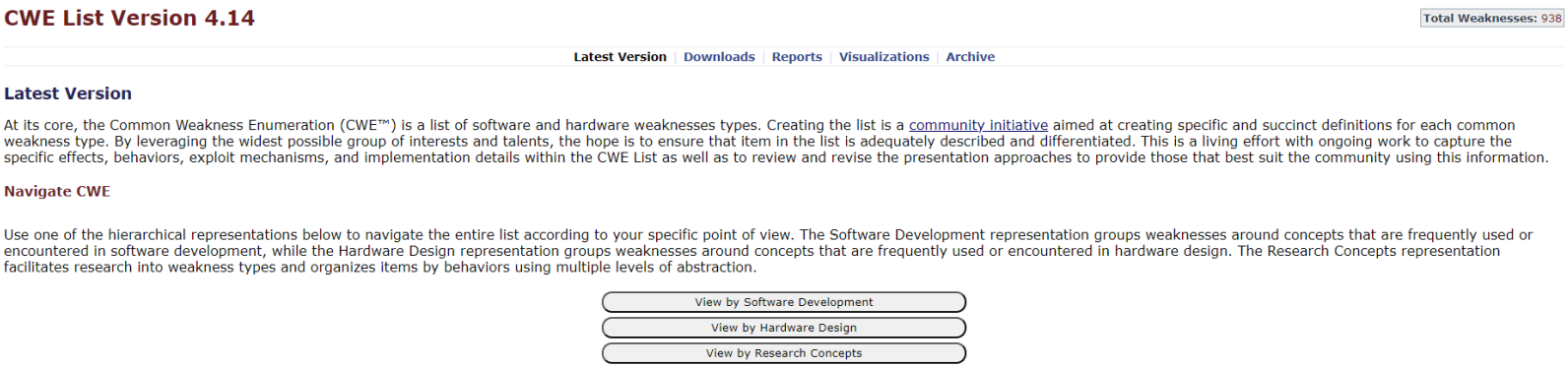
Tassonomia delle Vulnerabilità
Common Weakness Enumeration (CWE)

- CWE si basa sui seguenti punti chiave
  - **Categorizzazione delle debolezze**: CWE fornisce un elenco standardizzato delle «debolezze» comuni del software e dell'hardware
    - Ad ogni debolezza viene assegnato un identificatore univoco
  - **Comprensione delle debolezze**: CWE aiuta a comprendere le cause delle vulnerabilità, organizzandole in classi diverse e fornendo descrizioni dettagliate per ciascuna debolezza
  - **Prevenzione delle debolezze**: CWE punta a migliorare la sicurezza del software e dell'hardware aiutando a prevenire, identificare ed affrontare le vulnerabilità comuni

Tassonomia delle Vulnerabilità

CWE - Interfaccia

- **https://cwe.mitre.org/data/index.html**



CWE List Version 4.14

Total Weaknesses: 938

Latest Version | Downloads | Reports | Visualizations | Archive

Latest Version

At its core, the Common Weakness Enumeration (CWE™) is a list of software and hardware weaknesses types. Creating the list is a community initiative aimed at creating specific and succinct definitions for each common weakness type. By leveraging the widest possible group of interests and talents, the hope is to ensure that item in the list is adequately described and differentiated. This is a living effort with ongoing work to capture the specific effects, behaviors, exploit mechanisms, and implementation details within the CWE List as well as to review and revise the presentation approaches to provide those that best suit the community using this information.

Navigate CWE

Use one of the hierarchical representations below to navigate the entire list according to your specific point of view. The Software Development representation groups weaknesses around concepts that are frequently used or encountered in software development, while the Hardware Design representation groups weaknesses around concepts that are frequently used or encountered in hardware design. The Research Concepts representation facilitates research into weakness types and organizes items by behaviors using multiple levels of abstraction.

View by Software Development

View by Hardware Design

View by Research Concepts

Tassonomia delle Vulnerabilità

CWE – External Mappings

- **https://cwe.mitre.org/data/index.html**

External Mappings

These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor.

- CWE Top 25 (2023)
- Most Important Hardware Weaknesses List (2021)
- OWASP Top Ten (2021)
- Seven Pernicious Kingdoms
- Software Fault Pattern Clusters
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT Perl Coding Standard
- Addressed by ISA/IEC 62443 Requirements
- CISQ Quality Measures (2020)
- CISQ Data Protection Measures
- SEI ETF Security Vulnerabilities in ICS
- Architectural Concepts

Tassonomia delle Vulnerabilità

CWE – Helpful Views

- **https://cwe.mitre.org/data/index.html**

Helpful Views

A number of additional helpful views have been created. These are based on a specific criteria and hope to provide insight for a certain domain or use case.

- Introduced During Design
- Introduced During Implementation
- Software Assurance Trends Categorization
- Quality Weaknesses with Indirect Security Impacts
- Software Written in C
- Software Written in C++
- Software Written in Java
- Software Written in PHP
- Weaknesses in Mobile Applications
- CWE Composites
- CWE Named Chains
- CWE Cross-Section
- CWE Simplified Mapping
- CWE Entries with Maintenance Notes
- CWE Deprecated Entries
- CWE Comprehensive View
- Weakness Base Elements

Tassonomia delle Vulnerabilità

CWE – Downloads

- **https://cwe.mitre.org/data/downloads.html**

Downloads

XML Content	Published	Schema	Documentation
ZIP	PDF	XSD	HTML

The following tables contains alternative formats for viewing the CWE List. The options are:

- **Booklet.html**: A webpage containing the rendered HTML representation of the desired CWE ID, and all dependent Weaknesses, Views, or Categories.
- **CSV.zip**: A compressed CSV file containing the fields of the desired Weaknesses related to this View.
- **XML.zip**: A compressed XML file containing the desired CWE ID, dependent Weaknesses, Views, Categories, and all required External References.

Navigate CWE

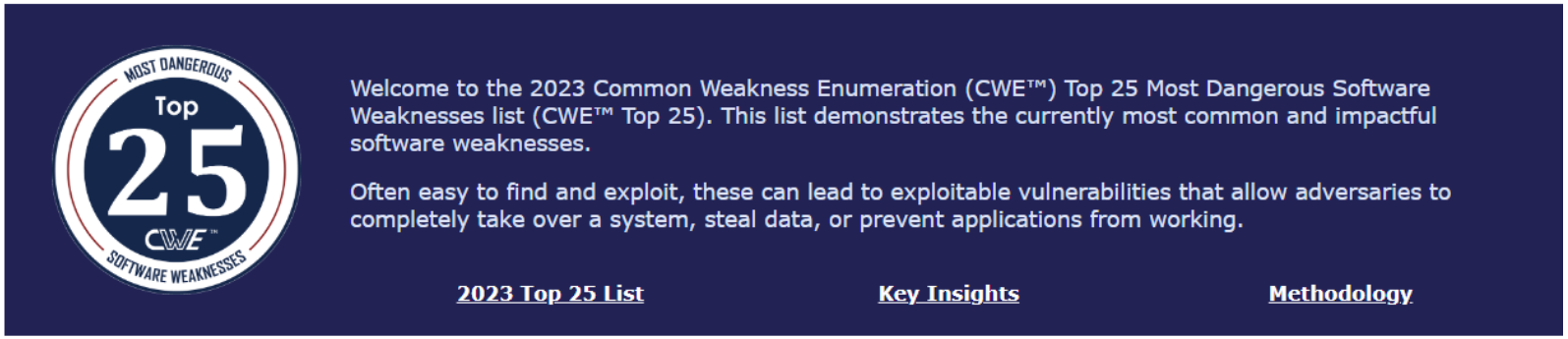
Software Development	Booklet.html	CSV.zip	XML.zip
Hardware Design	Booklet.html	CSV.zip	XML.zip
Research Concepts	Booklet.html	CSV.zip	XML.zip

Tassonomia delle Vulnerabilità

CWE – Top 25

- https://cwe.mitre.org/top25/

CWE Top 25 Most Dangerous Software Weaknesses



Tassonomia delle Vulnerabilità

CWE – Top 25

- https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

2023 CWE Top 25 Most Dangerous Software Weaknesses

Top 25 Home | Share via: | View in table format | Key Insights | Methodology

1. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1
2. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3
4. Use After Free
   CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲
5. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
   CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲
6. Improper Input Validation
   CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼

Tassonomia delle Vulnerabilità

CWE – Most Important Hardware Weaknesses (MIHW)

- **https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html**

The 2021 CWE™ Most Important Hardware Weaknesses is the first of its kind and the result of collaboration within the Hardware CWE Special Interest Group (SIG), a community forum for individuals representing organizations within hardware design, manufacturing, research, and security domains, as well as academia and government.

The goals for the 2021 Hardware List are to drive awareness of common hardware weaknesses through CWE, and to prevent hardware security issues at the source by educating designers and programmers on how to eliminate important mistakes early in the product development lifecycle. Security analysts and test engineers can use the list in preparing plans for security testing and evaluation. Hardware consumers could use the list to help them to ask for more secure hardware products from their suppliers. Finally, managers and CIOs can use the list as a measuring stick of progress in their efforts to secure their hardware and ascertain where to direct resources to develop security tools or automation processes that mitigate a wide class of vulnerabilities by eliminating the underling root cause.

MITRE maintains the CWE web site with the support of the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), presenting detailed descriptions of the 2021 Hardware List weaknesses along with authoritative guidance for mitigating and avoiding them. The CWE site contains data on more than 900 programming, design, and architecture weaknesses that can lead to exploitable vulnerabilities. MITRE also publishes the CWE Top-25 Most Dangerous Software Weaknesses on an annual basis.

CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

Tassonomia delle Vulnerabilità

CWE – Top 10 KEV Weaknesses

- https://cwe.mitre.org/top25/archive/2023/2023_kev_list.html

2023 CWE Top 10 KEV Weaknesses

Top 25 Home | Share via: | View in table format | KEV Key Insights | KEV Methodology

1	Use After Free	CWE-416 | Analysis score: 73.99 | # CVE Mappings in KEV: 44 | Avg. CVSS: 8.54
2	Heap-based Buffer Overflow	CWE-122 | Analysis score: 56.56 | # CVE Mappings in KEV: 32 | Avg. CVSS: 8.79
3	Out-of-bounds Write	CWE-787 | Analysis score: 51.96 | # CVE Mappings in KEV: 34 | Avg. CVSS: 8.19
4	Improper Input Validation	CWE-20 | Analysis score: 51.38 | # CVE Mappings in KEV: 33 | Avg. CVSS: 8.27
5	Improper Neutralization of Special Elements used in an OS Command	CWE-78 | Analysis score: 49.44 | # CVE Mappings in KEV: 25 | Avg. CVSS: 9.36
6	Deserialization of Untrusted Data	CWE-502 | Analysis score: 29.00 | # CVE Mappings in KEV: 16 | Avg. CVSS: 9.06

Tassonomia delle Vulnerabilità

Common Attack Pattern Enumeration and Classification (CAPEC) – Caratteristiche

- Risorsa collaborativa che consente di identificare e comprendere gli attacchi
- Fornisce un **catalogo** pubblicamente disponibile di **attack pattern comuni** che consente di capire come gli attaccanti sfruttano le debolezze rilevate
- Gli attack pattern
  - Descrivono gli approcci comunemente utilizzati per sfruttare determinate debolezze
  - Definiscono le sfide che un avversario deve affrontare durante un attacco
  - Derivano dal concetto di *design pattern*, applicato in un contesto distruttivo piuttosto che costruttivo
  - Sono generati a partire da un'analisi approfondita di specifici attacchi che avvengono nel mondo reale

Tassonomia delle Vulnerabilità

Common Attack Pattern Enumeration and Classification (CAPEC) – Caratteristiche

- Ogni attack pattern raccoglie/mostra informazioni su come vengono progettate ed eseguite parti specifiche di un attacco e fornisce indicazioni su come mitigare l'efficacia dell'attacco
- Gli attack pattern aiutano a comprendere meglio gli elementi specifici di un attacco e come impedirne la riuscita
- CAPEC è stato istituito dal *U.S. Department of Homeland Security* come parte dell'iniziativa strategica *Software Assurance* (*SwA*) dell'*Office of Cybersecurity and Communications* (*CS&C*)

Tassonomia delle Vulnerabilità

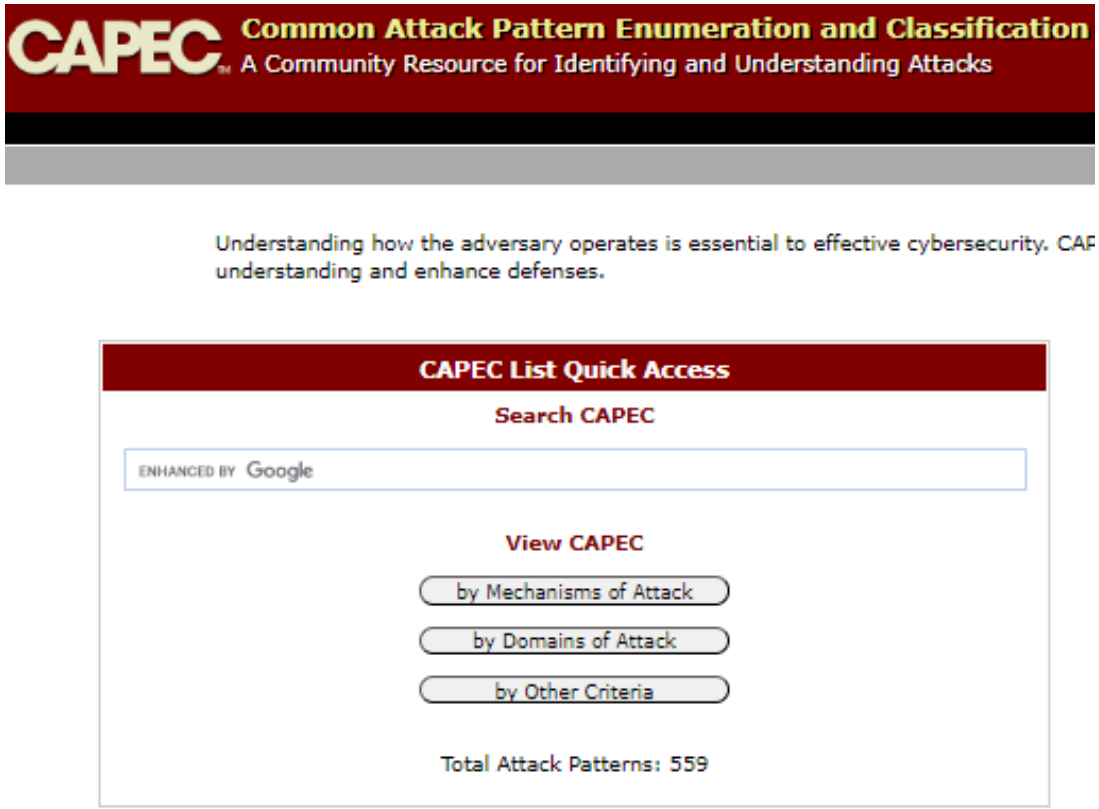
Common Attack Pattern Enumeration and Classification (CAPEC) – Caratteristiche

- Il CAPEC è relato al **C**ommon **W**eakness **E**numeration (**CWE**) ed al **C**ommon **V**ulnerabilities and **E**xposures (CVE)
- Un attack pattern definito nel CAPEC è tipicamente un metodo per sfruttare uno o più CWE al fine di eseguire un attacco
- Molte entry del CAPEC contengono un **`Execution Flow`**
  - Istruzioni dettagliate su come un avversario può sfruttare una debolezza (CWE)

Tassonomia delle Vulnerabilità

Common Attack Pattern Enumeration and Classification (CAPEC) – Interfaccia

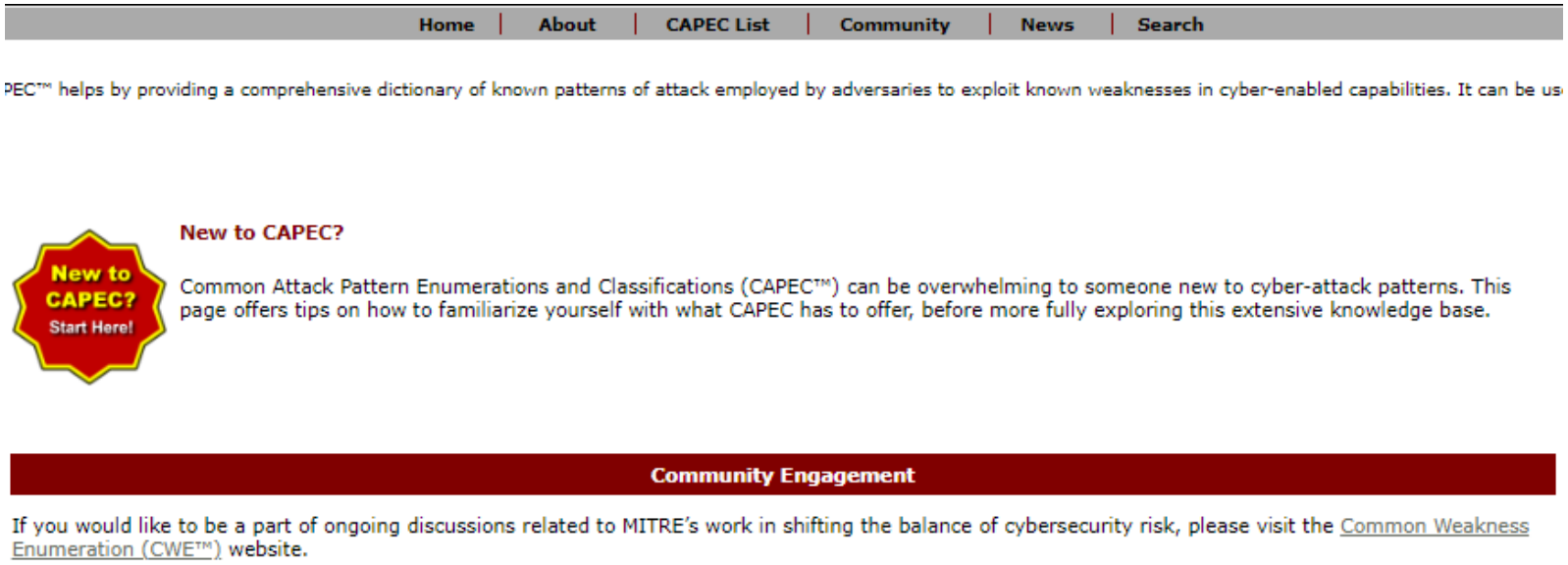
- **https://capec.mitre.org/**



Tassonomia delle Vulnerabilità

Common Attack Pattern Enumeration and Classification (CAPEC) – Interfaccia

- **https://capec.mitre.org/**



Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Ad ogni entry del CAPEC è associato un ID numerico (**`Attack Pattern ID`**)
  - L'ID non codifica alcuna informazione in particolare, ma serve solo a indicare quando la entry è stata aggiunta al CAPEC
- Tutte le entry hanno anche un titolo ed una descrizione
  - Una descrizione è un riepilogo di ciò che riguarda l'attack pattern

CAPEC-36: Using Unpublished Interfaces

Attack Pattern ID: 36 **Status:** Draft

Description

An adversary searches for and invokes interfaces that the target system designers did not intend to be publicly available. If these interfaces fail to authenticate requests the attacker may be able to invoke functionality they are not authorized for.

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Le debolezze sfruttate dall'attack pattern sono elencate nella sezione **`Related Weaknesses`**
- Si noti che la mappatura tra le entry del CAPEC e le debolezze del CWE non segue necessariamente una relazione uno-a-uno
- L'attack pattern potrebbe dover sfruttare tutte le debolezze elencate, un sottoinsieme di esse o solo una
  - Spesso esistono diverse debolezze, ognuna delle quali potrebbe essere utilizzata per consentire l'exploitation di una determinata vulnerabilità

Related Weaknesses

CWE-ID	Weakness Name
306	Missing Authentication for Critical Function
693	Protection Mechanism Failure
695	Use of Low-Level Functionality

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- L'**`Execution Flow`** fornisce istruzioni esaustive su come eseguire l'attacco

Execution Flow

Explore

1. **Identify services:** Discover a service of interest by exploring service registry listings or by connecting on a known port or some similar means.

Techniques
Search via internet for known, published services.
Use automated tools to scan known ports to identify internet-enabled services.
Dump the code from the chip and then perform reverse engineering to analyze the code.

2. **Authenticate to service:** Authenticate to the service, if required, in order to explore it.

Techniques
Use published credentials to access system.
Find unpublished credentails to access service.
Use other attack pattern or weakness to bypass authentication.

3. **Identify all interfaces:** Determine the exposed interfaces by querying the registry as well as probably sniffing to expose interfaces that are not explicitly listed.

Techniques
For any published services, determine exposed interfaces via the documentation provided.
For any services found, use error messages from poorly formed service calls to determine valid interfaces. In some cases, services will respond to poorly formed calls with valid ones.

Experiment

1. **Attempt to discover unpublished functions:** Using manual or automated means, discover unpublished or undocumented functions exposed by the service.

Techniques
Manually attempt calls to the service using an educated guess approach, including the use of terms like' 'test', 'debug', 'delete', etc.
Use automated tools to scan the service to attempt to reverse engineer exposed, but undocumented, features.

Exploit

1. **Exploit unpublished functions:** Using information determined via experimentation, exploit the unpublished features of the service.

Techniques
Execute features that are not intended to be used by general system users.
Craft malicious calls to features not intended to be used by general system users that take advantage of security flaws found in the functions.

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Un **`Execution flow`** è tipicamente costituito da tre fasi
  - **`Explore`**: Questa fase descrive vari modi per trovare un potenziale obiettivo da attaccare
  - **`Experiment`**: Una volta trovato un obiettivo, questa fase suggerisce vari modi per determinare se tale obiettivo contiene debolezze da sfruttare
  - **`Exploit`**: Tecniche suggerite per condurre l'attacco vero e proprio

- L'**`Execution Flow`** non riguarda solo come eseguire l'attacco, ma anche come determinare se l'obiettivo individuato è vulnerabile

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Una entry CAPEC definisce anche i prerequisiti (**`Prerequisites`**), le competenze (**`Skills Required`**) e le risorse (**`Resources Required`**) che sono necessarie per condurre un attacco

Prerequisites

The architecture under attack must publish or otherwise make available services that clients can attach to, either in an unauthenticated fashion, or having obtained an authentication token elsewhere. The service need not be 'discoverable', but in the event it isn't it must have some way of being discovered by an attacker. This might include listening on a well-known port. Ultimately, the likelihood of exploit depends on discoverability of the vulnerable service.

Skills Required

[Level: Low]
A number of web service digging tools are available for free that help discover exposed web services and their interfaces. In the event that a web service is not listed, the attacker does not need to know much more in addition to the format of web service messages that they can sniff/monitor for.

Resources Required

None: No specialized resources are required to execute this type of attack. Web service digging tools may be helpful.

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Le conseguenze di un attacco riuscito utilizzando un determinato attack pattern sono elencate nella sezione **`Consequences`**

Consequences

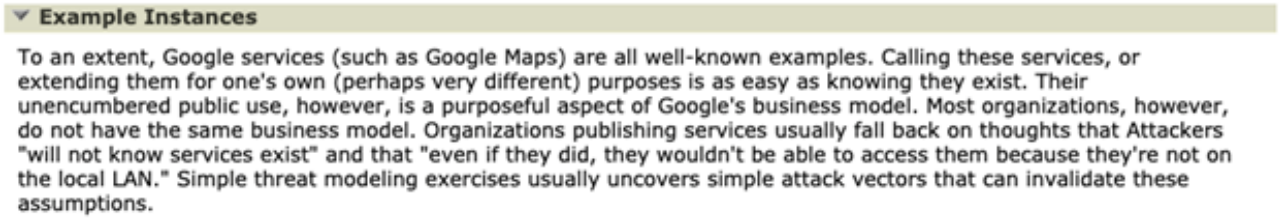
Scope	Impact
Confidentiality	Read Data
Confidentiality Access Control Authorization	Gain Privileges

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Esempio – CAPEC-36: Using Unpublished Interfaces or Functionality

- Gli esempi del mondo reale (**`Example Instances`**) sono spesso utili per capire come utilizzare un attack pattern



Example Instances

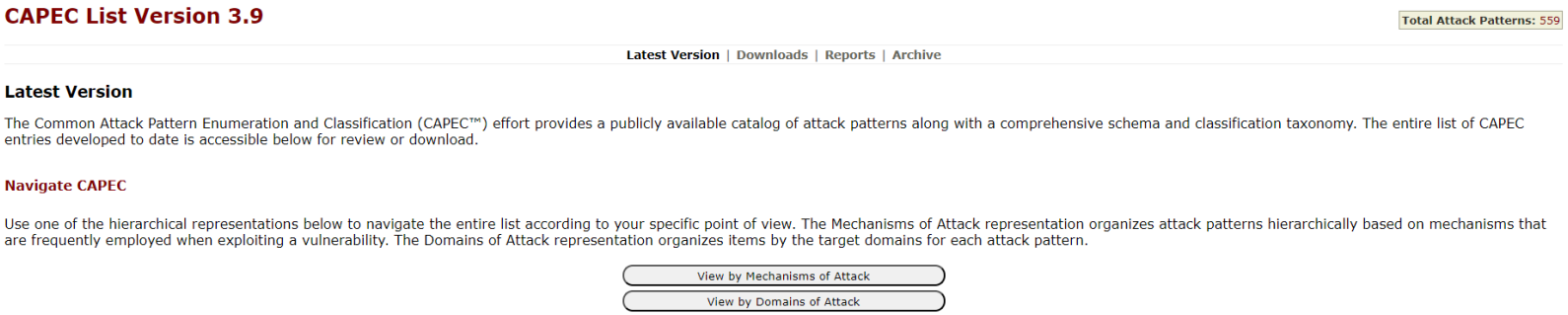
To an extent, Google services (such as Google Maps) are all well-known examples. Calling these services, or extending them for one's own (perhaps very different) purposes is as easy as knowing they exist. Their unencumbered public use, however, is a purposeful aspect of Google's business model. Most organizations, however, do not have the same business model. Organizations publishing services usually fall back on thoughts that Attackers "will not know services exist" and that "even if they did, they wouldn't be able to access them because they're not on the local LAN." Simple threat modeling exercises usually uncovers simple attack vectors that can invalidate these assumptions.

https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

CAPEC List Version 3.9

- https://capec.mitre.org/data/index.html



https://capec.mitre.org/data/definitions/36.html

Tassonomia delle Vulnerabilità

Ricapitolazione: CVE, CWE, CAPEC ed NVD

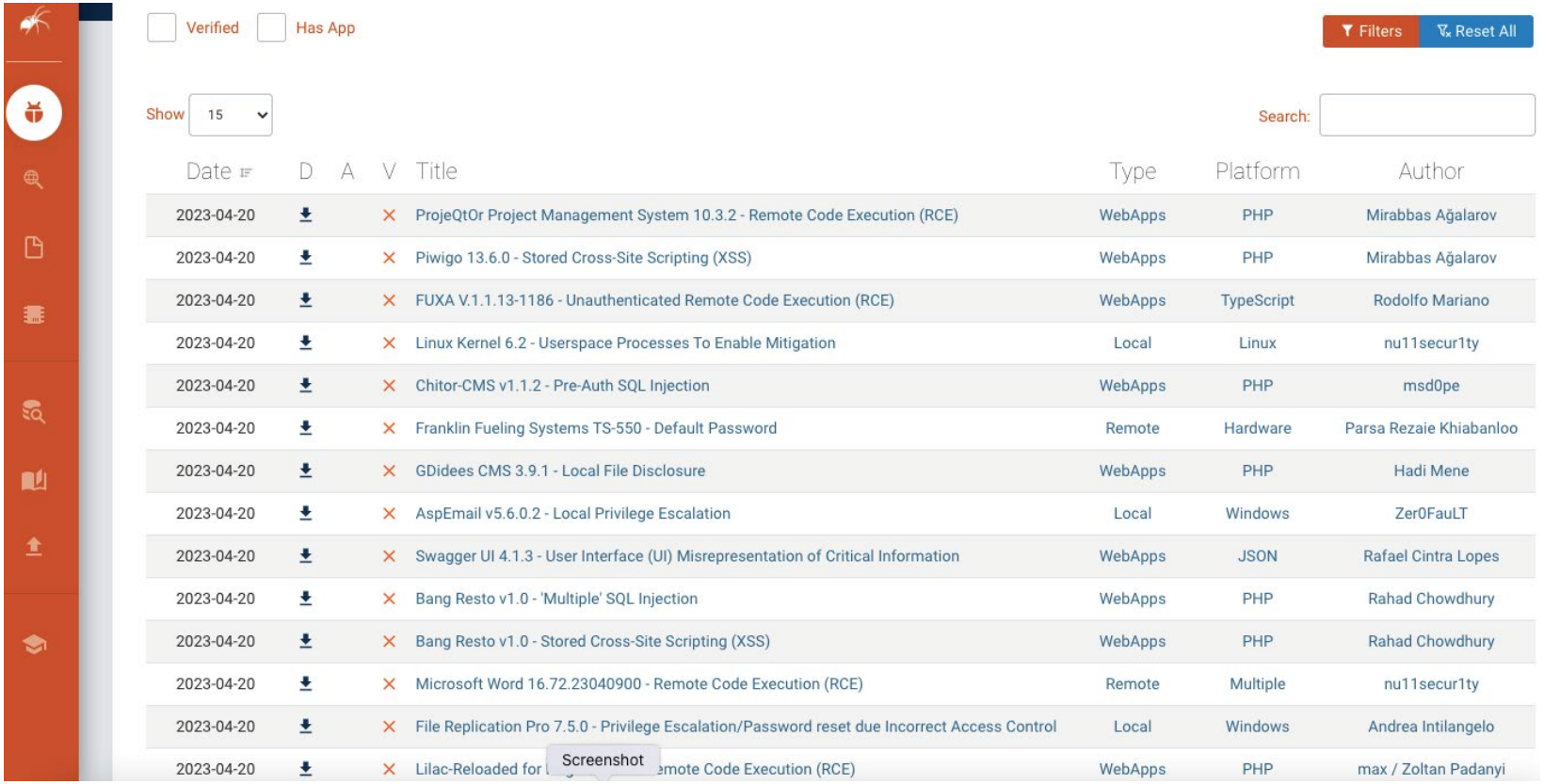
- **CVE**, **KEV**, **CWE**, **CAPEC** ed **NVD** sono componenti essenziali per la gestione delle vulnerabilità
  - **CVE** fornisce identificatori univoci per vulnerabilità specifiche
  - **KEV** fornisce indicazioni sulle vulnerabilità che sono state sfruttare
  - **CWE** classifica le debolezze comuni di software e hardware
  - **CAPEC** permette di identificare e capire i pattern di attacco più comuni
  - **NVD** funge da archivio centralizzato per le informazioni relative ai CVE

- Tali componenti aiutano a rimanere costantemente informati, comprendere e mitigare in modo efficace le vulnerabilità

Tassonomia delle Vulnerabilità

Altre Fonti – Exploit Database (EDB)

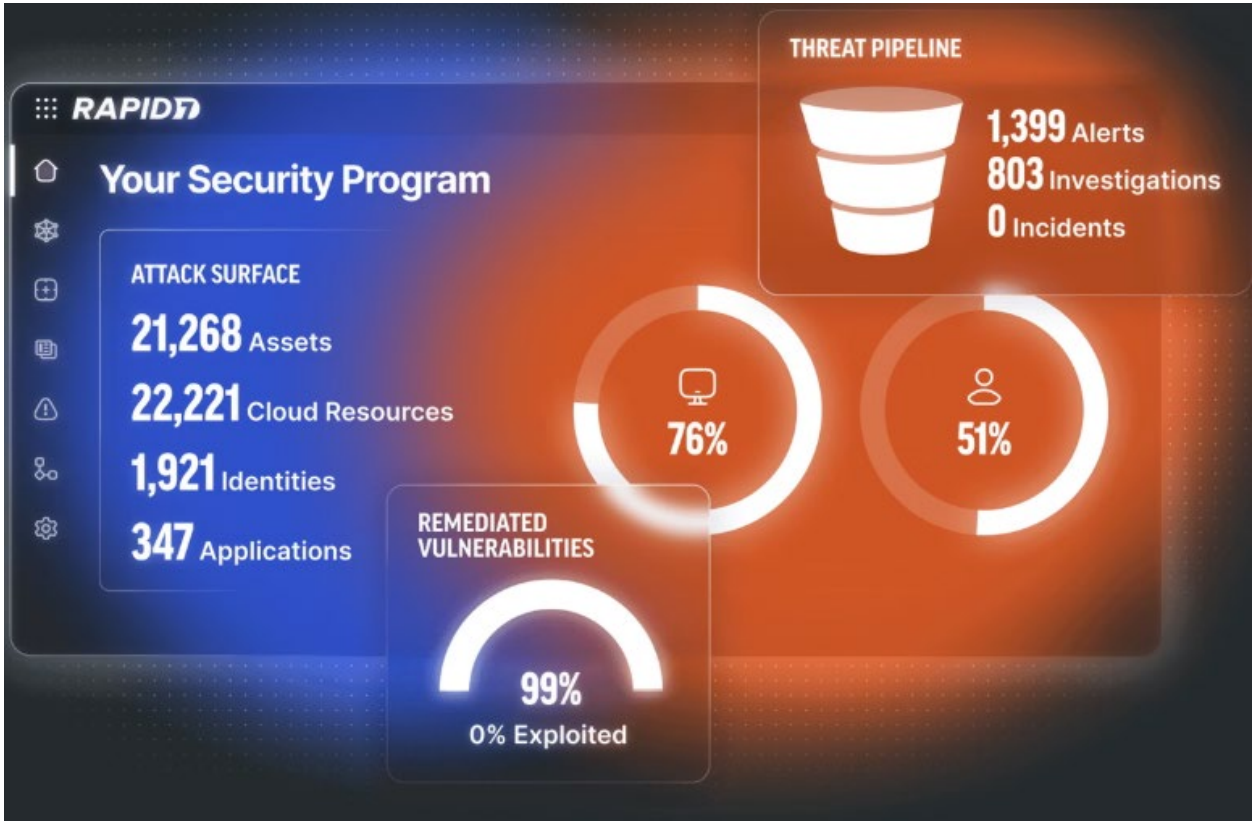
- **https://www.exploit-db.com/**



Tassonomia delle Vulnerabilità

Altre Fonti – RAPID7

- **https://www.rapid7.com/**



Tassonomia delle Vulnerabilità

Altre Fonti – Packet Storm

- **https://packetstormsecurity.com/**

Tassonomia delle Vulnerabilità

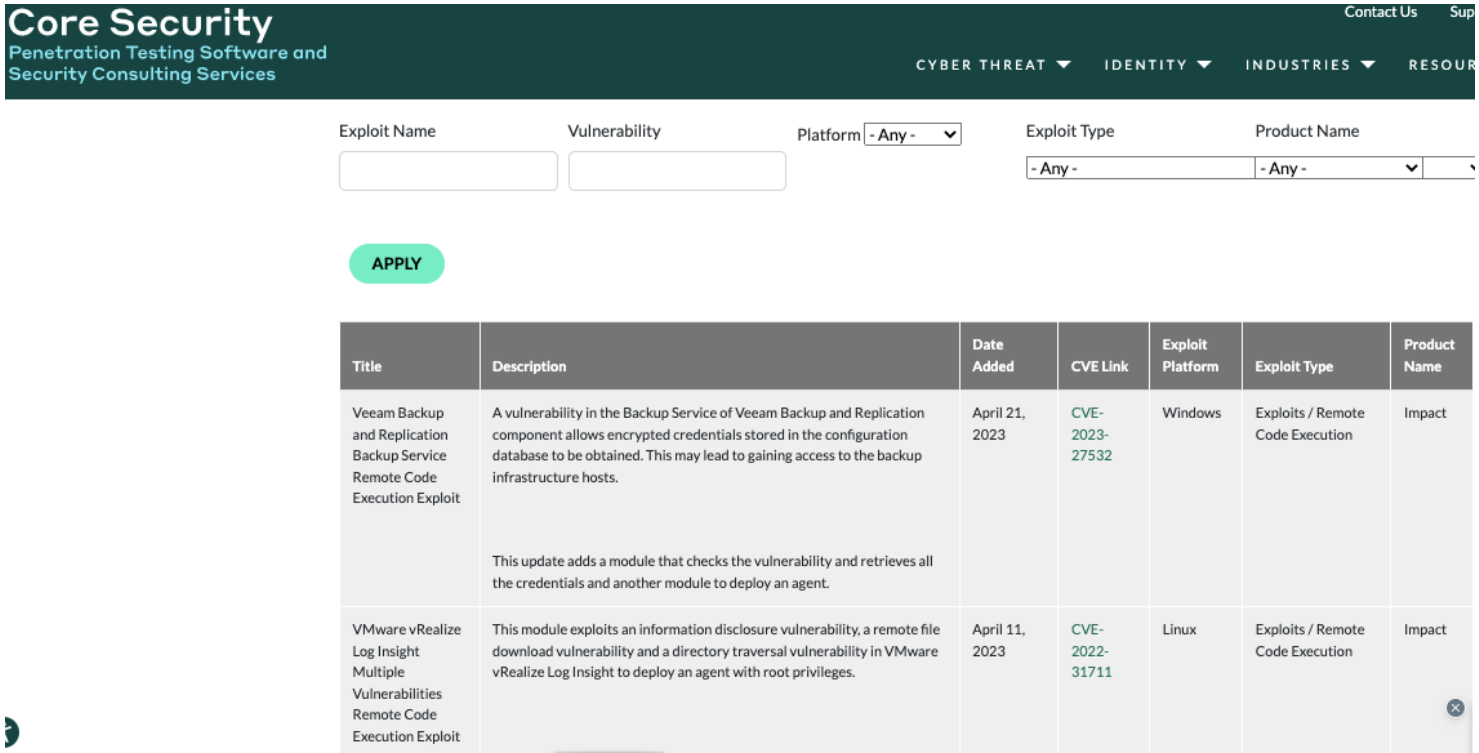
Altre Fonti – Flexera

- https://secuniaresearch.flexerasoftware.com/community/research/

Tassonomia delle Vulnerabilità

Altre Fonti – Core Security

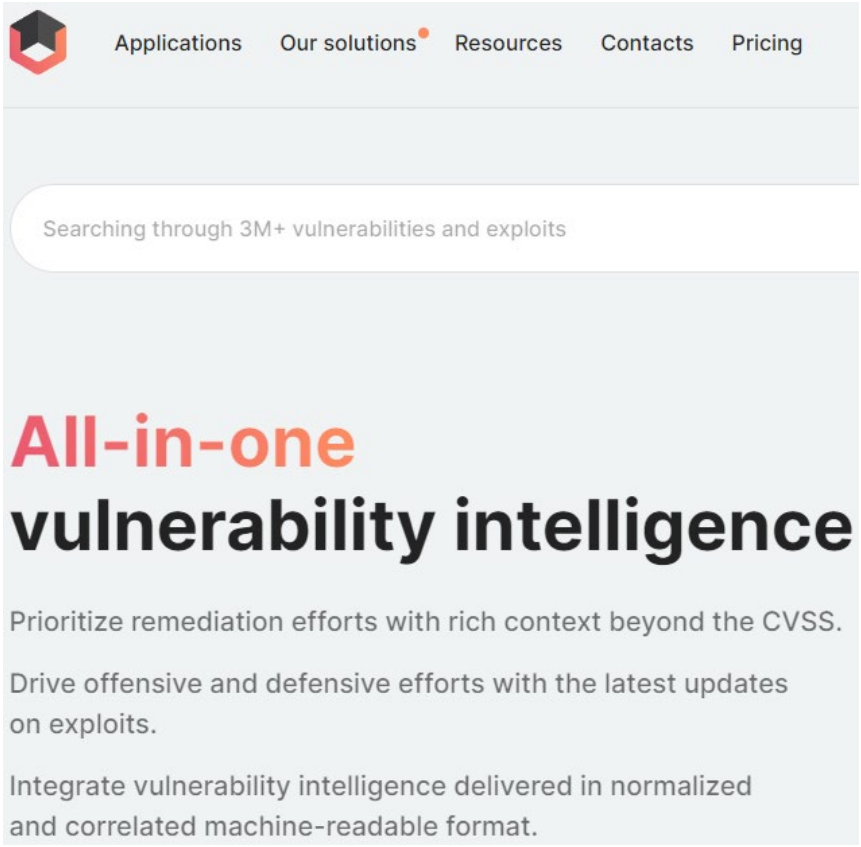
- **https://www.coresecurity.com/products/core-impact/recent-exploits-and-updates**



Tassonomia delle Vulnerabilità

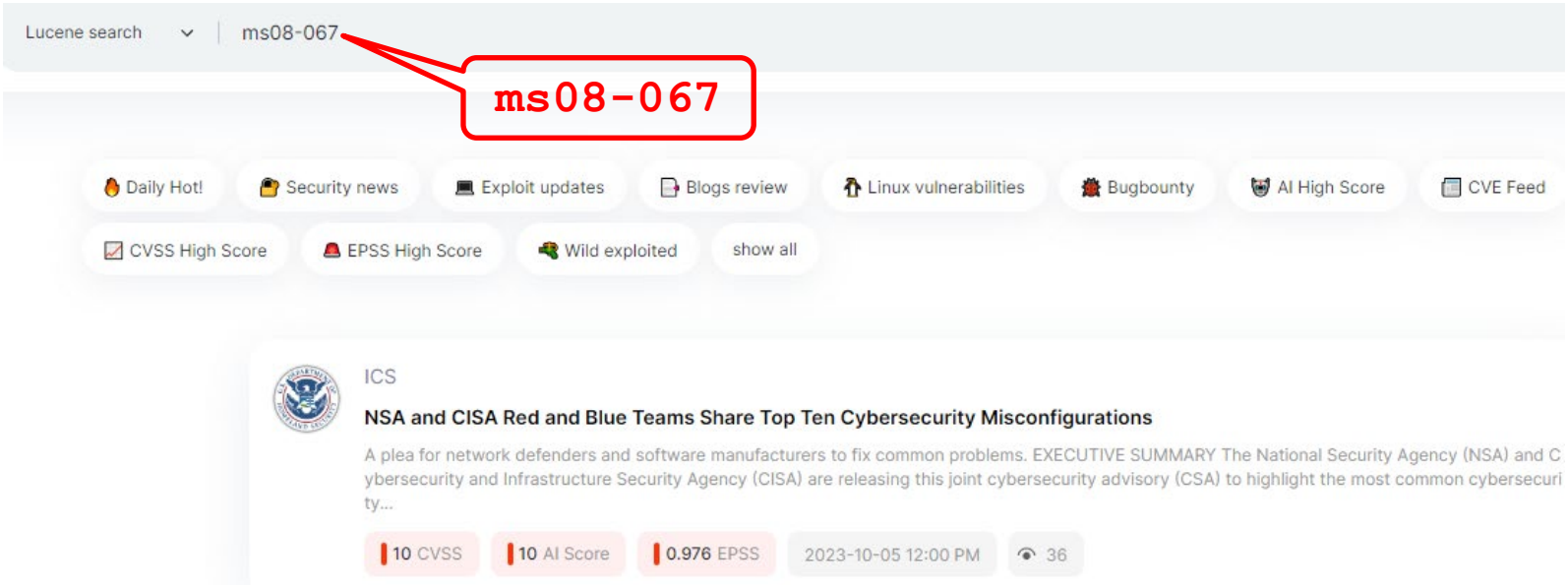
Altre Fonti – Vulners

- **https://vulners.com/**



Tassonomia delle Vulnerabilità

Altre Fonti – Vulners – Esempio



ms08-067

Outline

- Concetti Preliminari
- Caratterizzazione delle Vulnerabilità
- Tassonomia delle Vulnerabilità
- **Analisi Manuale delle Vulnerabilità**
- Analisi Automatica delle Vulnerabilità
- Analisi delle Vulnerabilità nelle Applicazioni Web
- Analisi delle Vulnerabilità nei Database

Analisi Manuale delle Vulnerabilità
Tipico Pattern

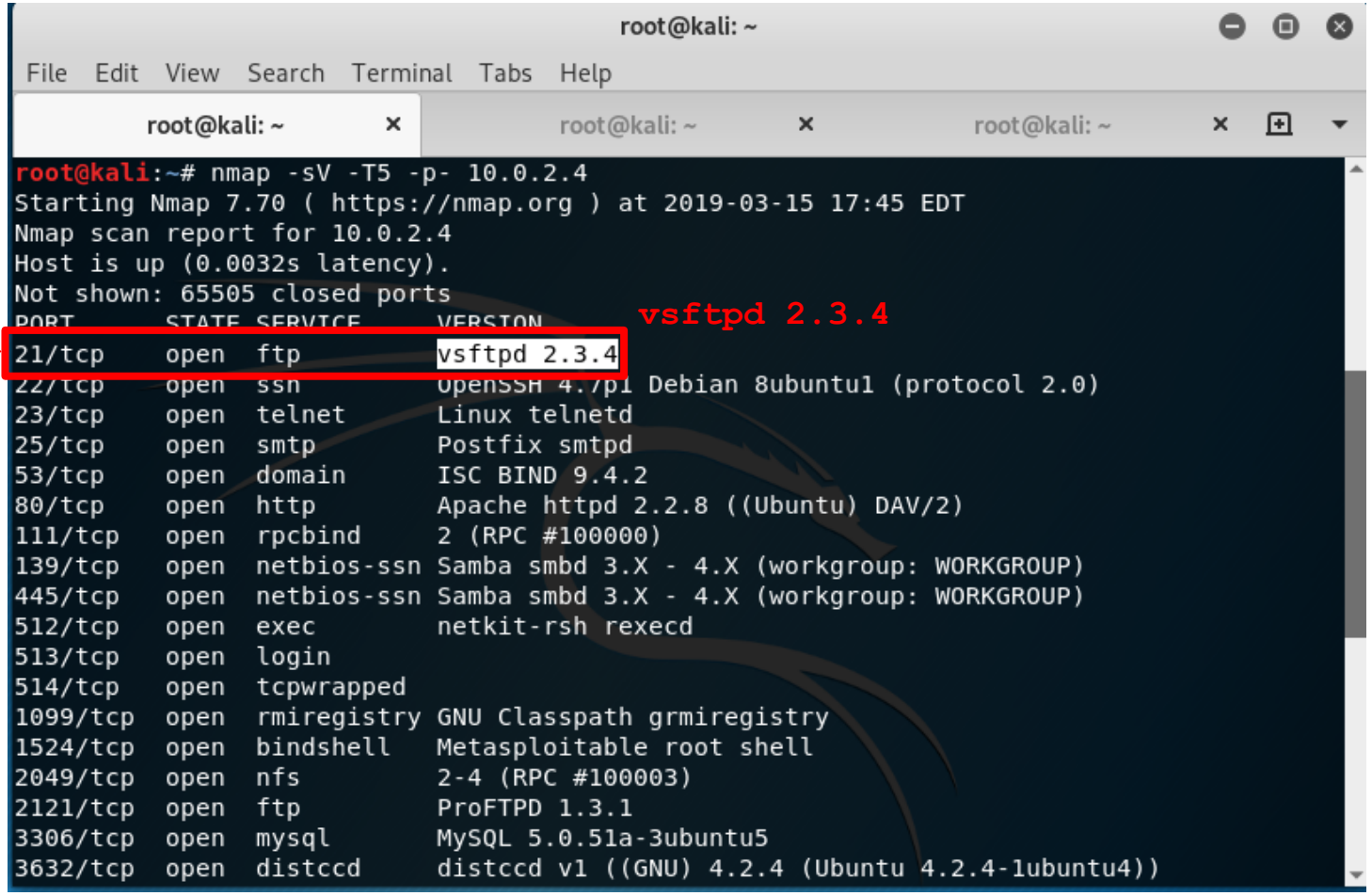
- Per l'analisi manuale delle vulnerabilità viene tipicamente utilizzato il seguente paradigma (o pattern)
  1. ***Active Service Enumeration*** sulla macchina target
     - Per rilevare la versione dei servizi che tale macchina espone
     - Fase di solito condotta usando strumenti come **`nmap`**
  2. ***Ricerca delle Vulnerabilità*** relative alla versione dei servizi rilevati
     - Fase tipicamente condotta tramite **ricerche manuali** sulle tassonomie delle vulnerabilità
       - In particolare sulla tassonomia denominata **E**xploit **D**ata**B**ase (**EDB**)
       - `https://www.exploit-db.com/`

Analisi Manuale delle Vulnerabilità
Esempio 1

- Utilizziamo il seguente ambiente operativo
  - **Macchina target:** Metasploitable 2 (Indirizzo IP: `10.0.2.4`)
  - Nmap per ottenere informazioni sui servizi di rete erogati dalla macchina target

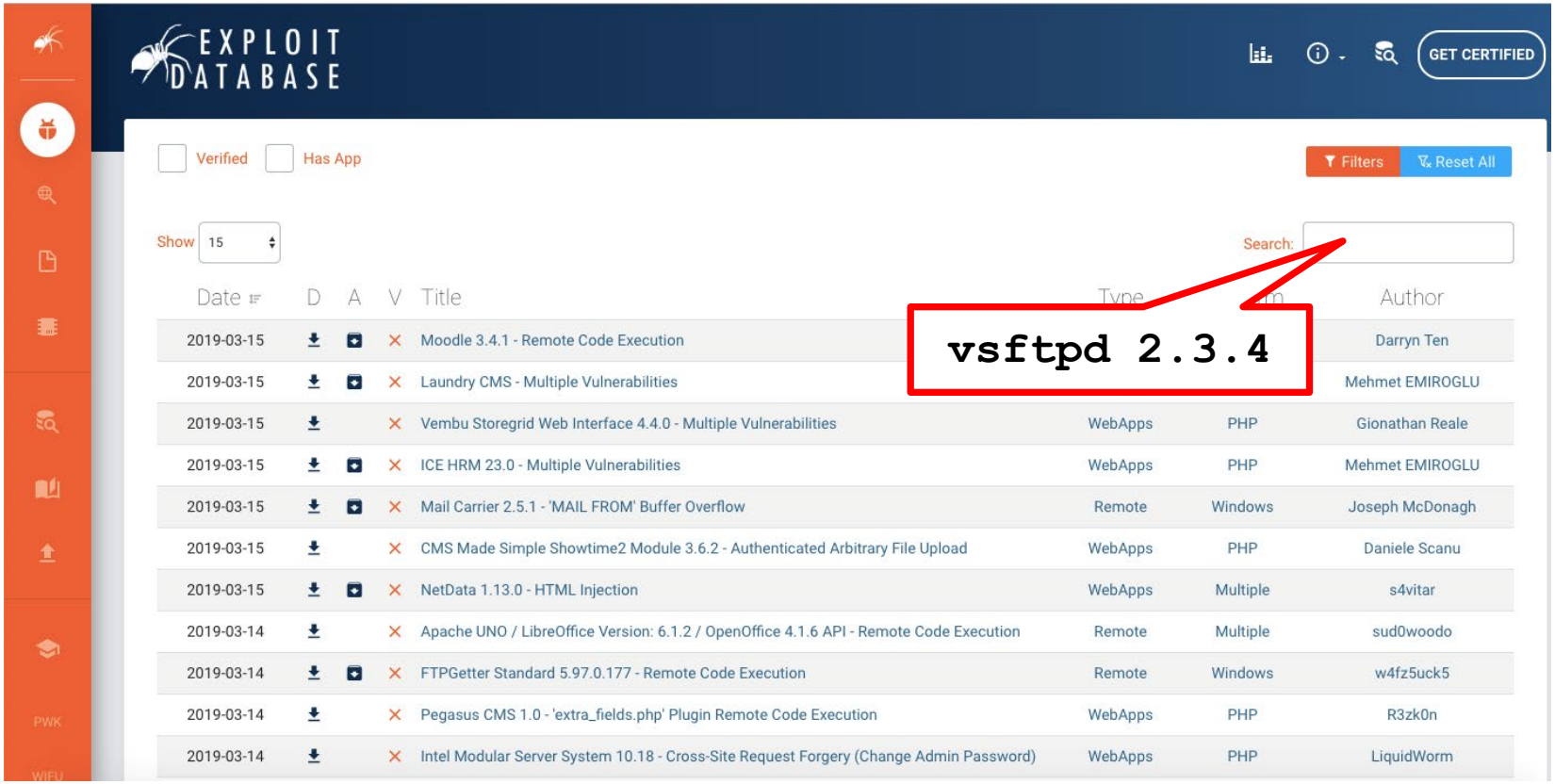
1. `nmap -sV -T5 -p- 10.0.2.4`
   - `-sV` permette di ottenere quante più informazioni possibili sul servizio erogato da ciascuna porta
   - `-T5` permette di ottenere la massima velocità di scansione
   - `-p-` permette di scansionare tutte le 2^{16} porte

Analisi Manuale delle Vulnerabilità
Esempio 1

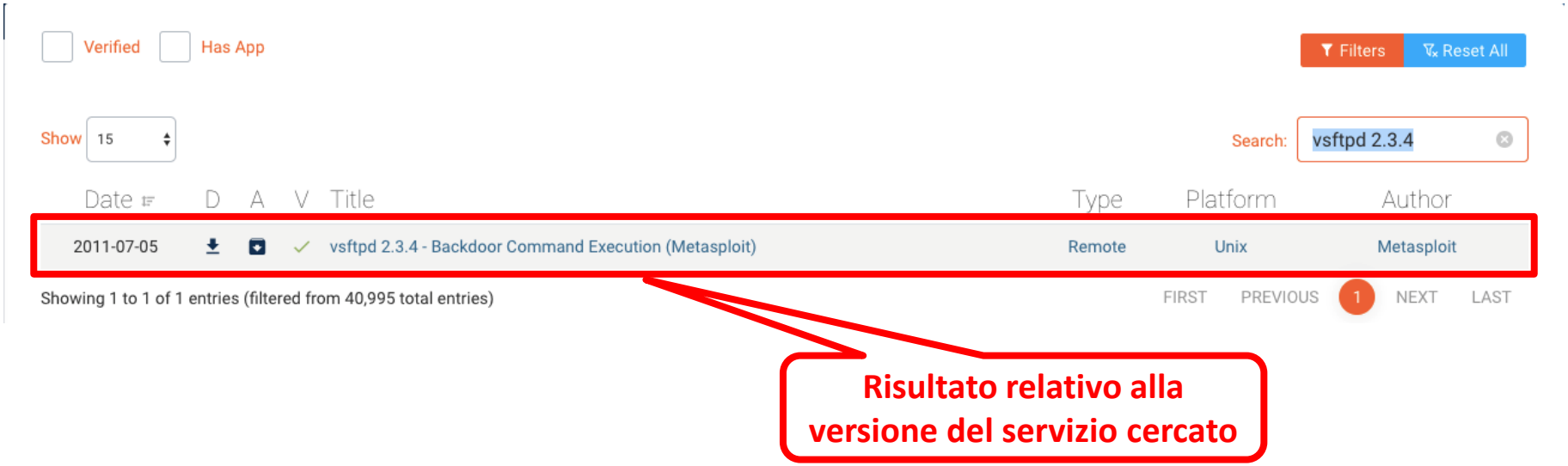


Analisi Manuale delle Vulnerabilità
Esempio 1

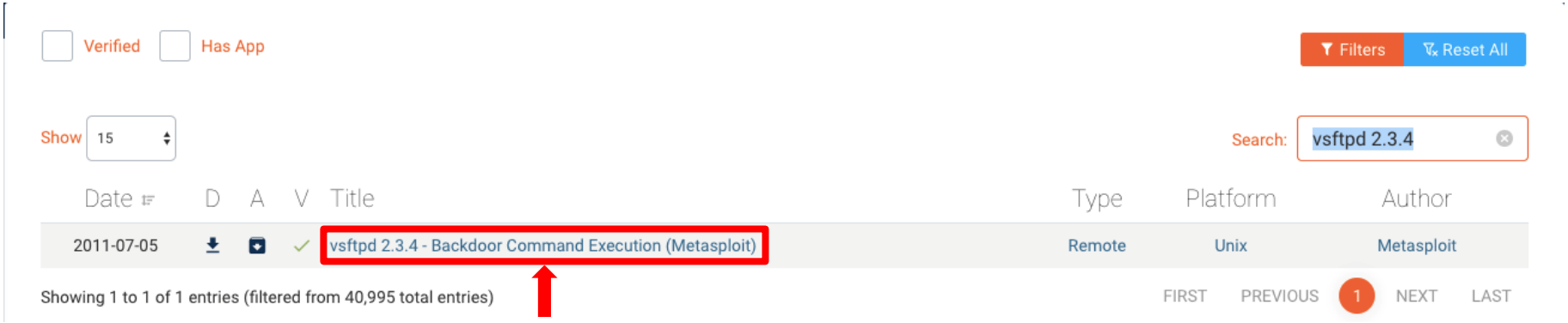
2. **https://www.exploit-db.com/**



Analisi Manuale delle Vulnerabilità
Esempio 1

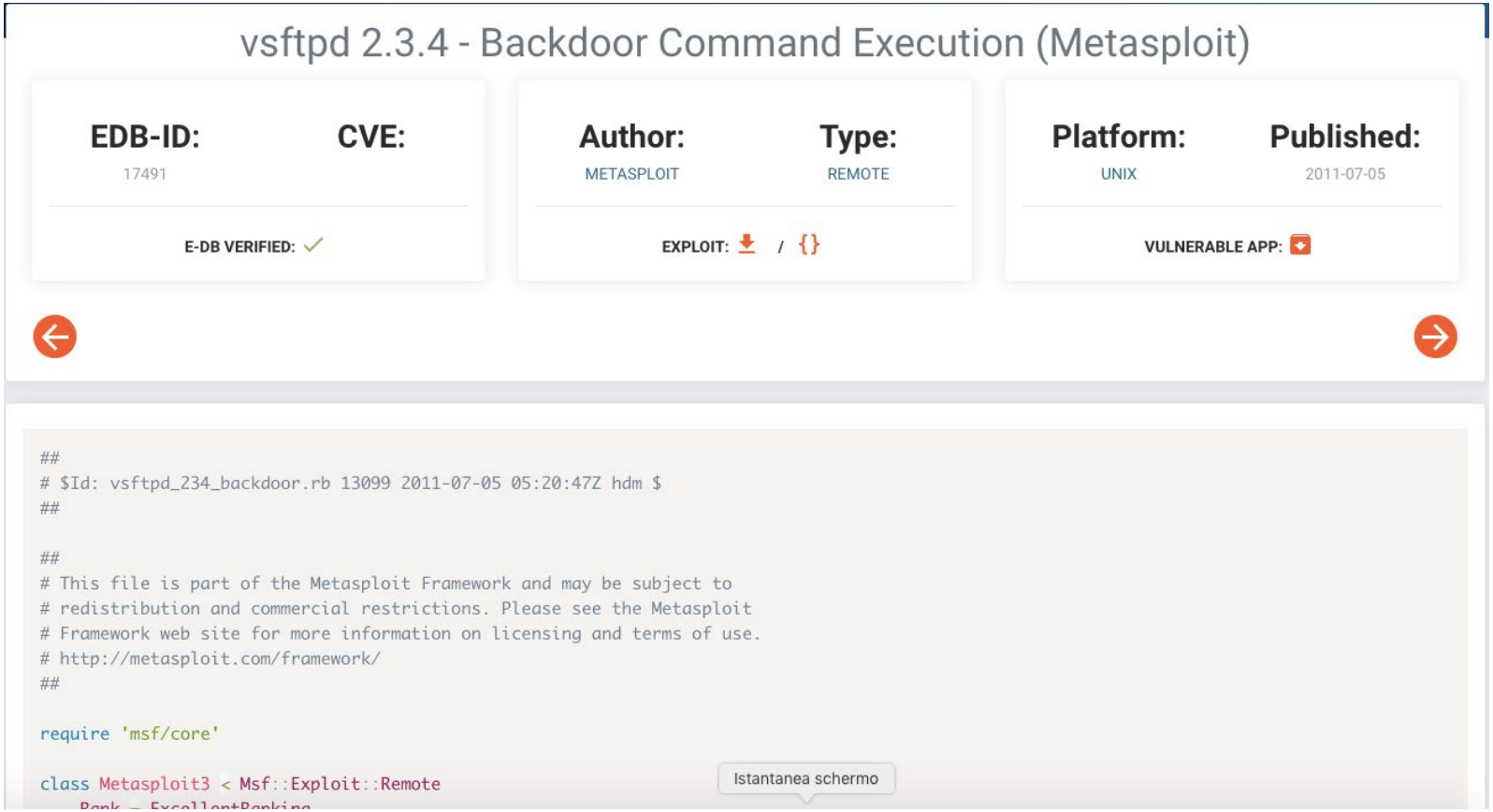


Analisi Manuale delle Vulnerabilità
Esempio 1

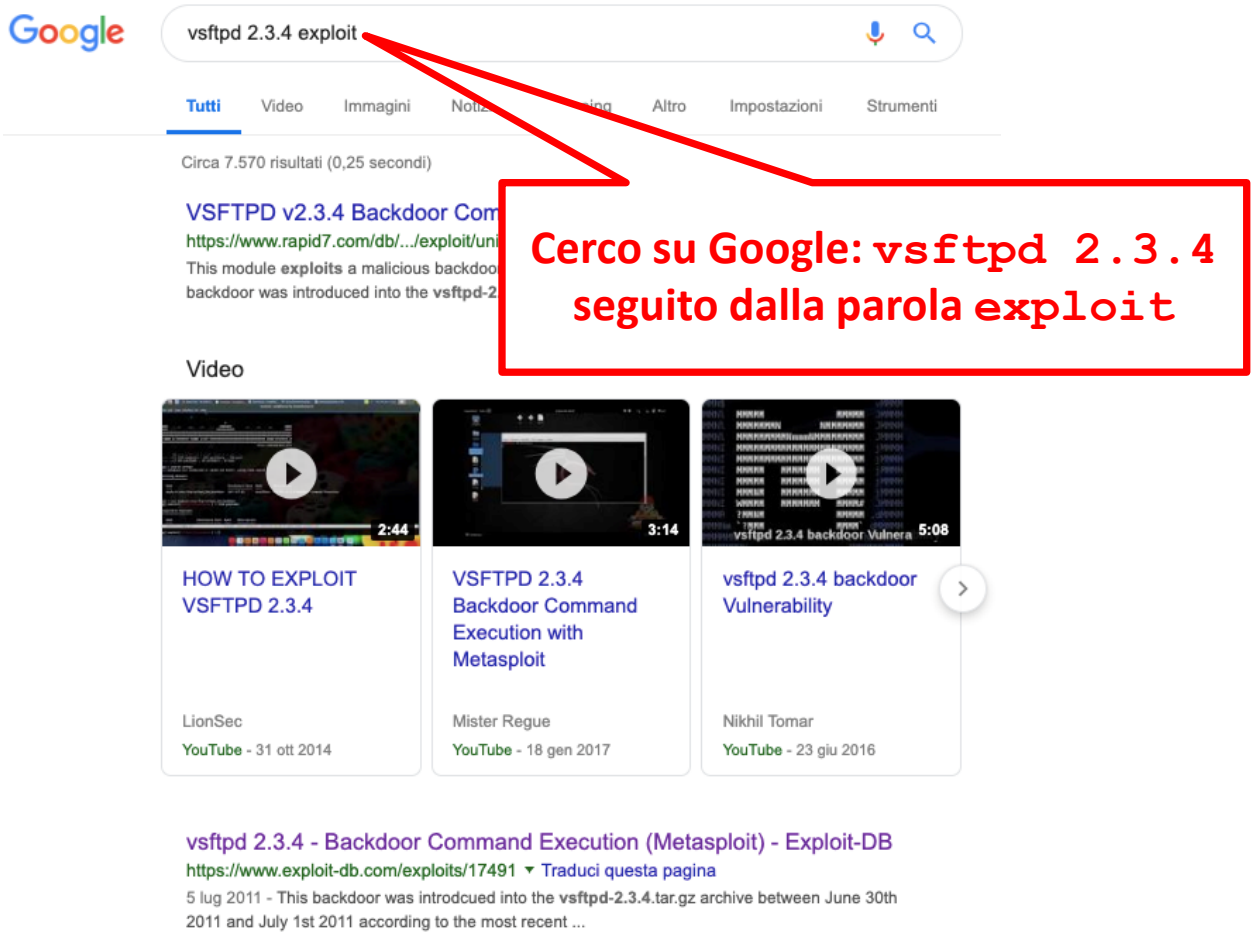


Seleziono il risultato trovato

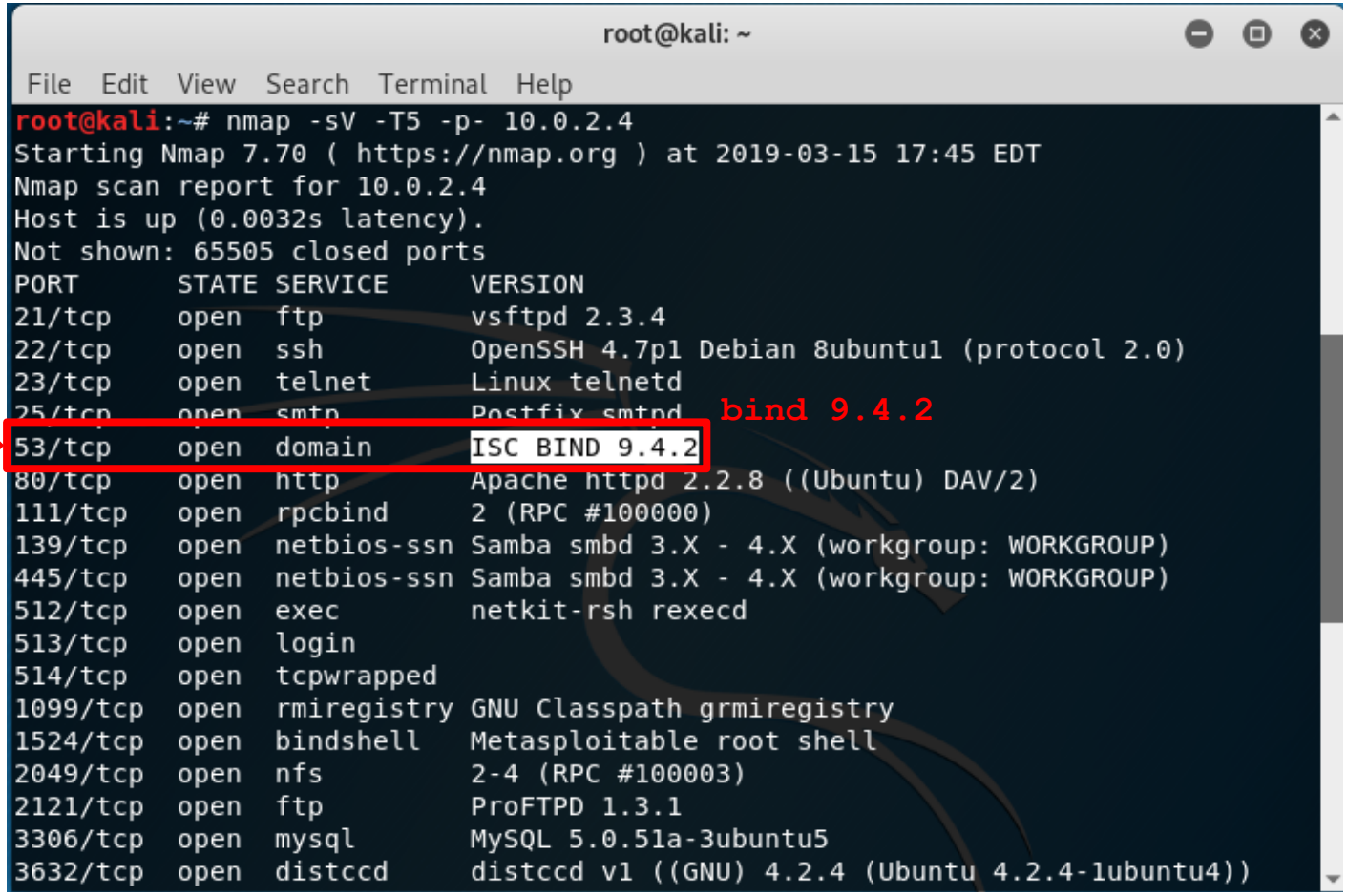
Analisi Manuale delle Vulnerabilità
Esempio 1



Analisi Manuale delle Vulnerabilità
Esempio 1 (Approccio Alternativo)

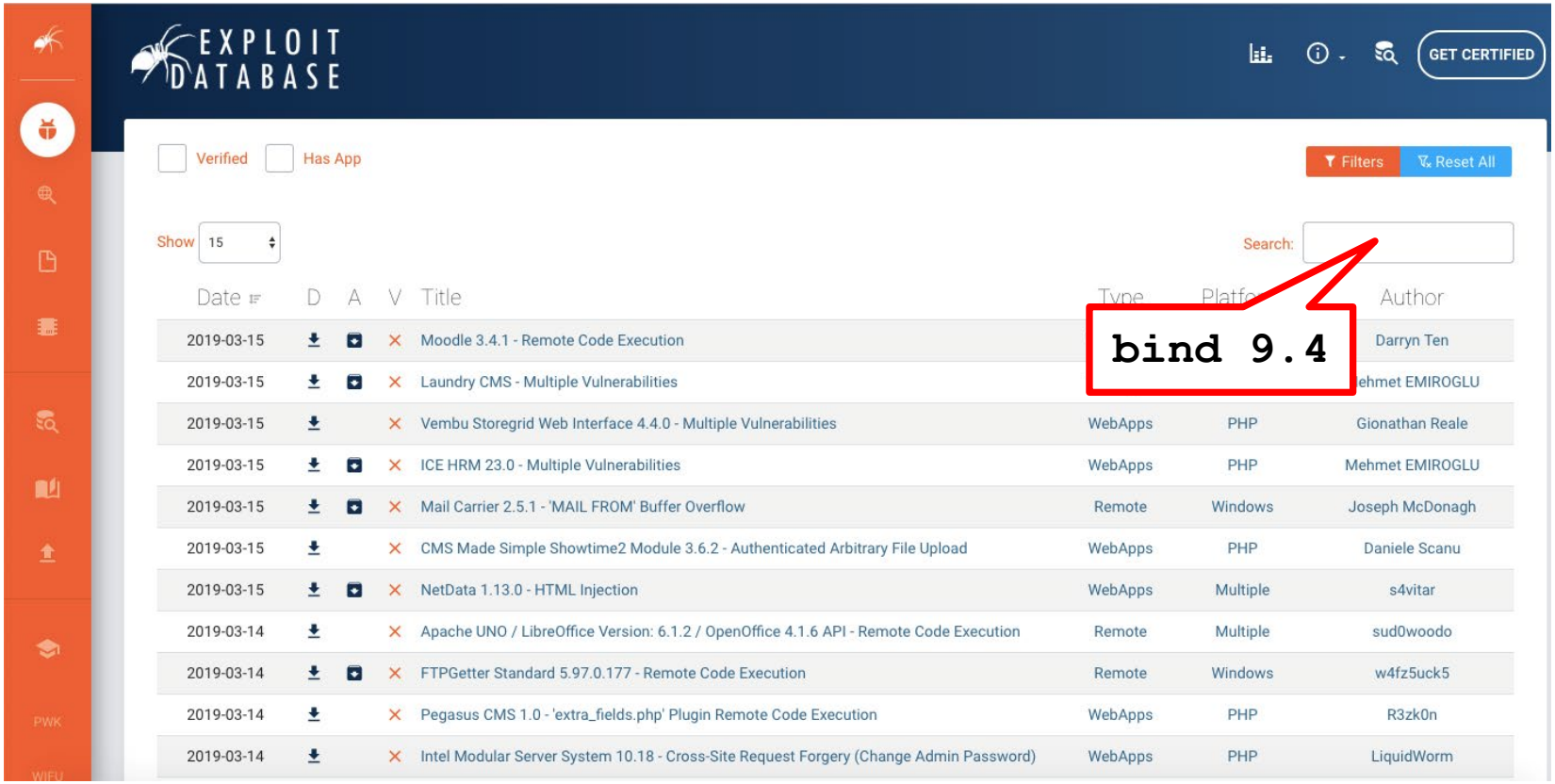


Analisi Manuale delle Vulnerabilità
Esempio 2

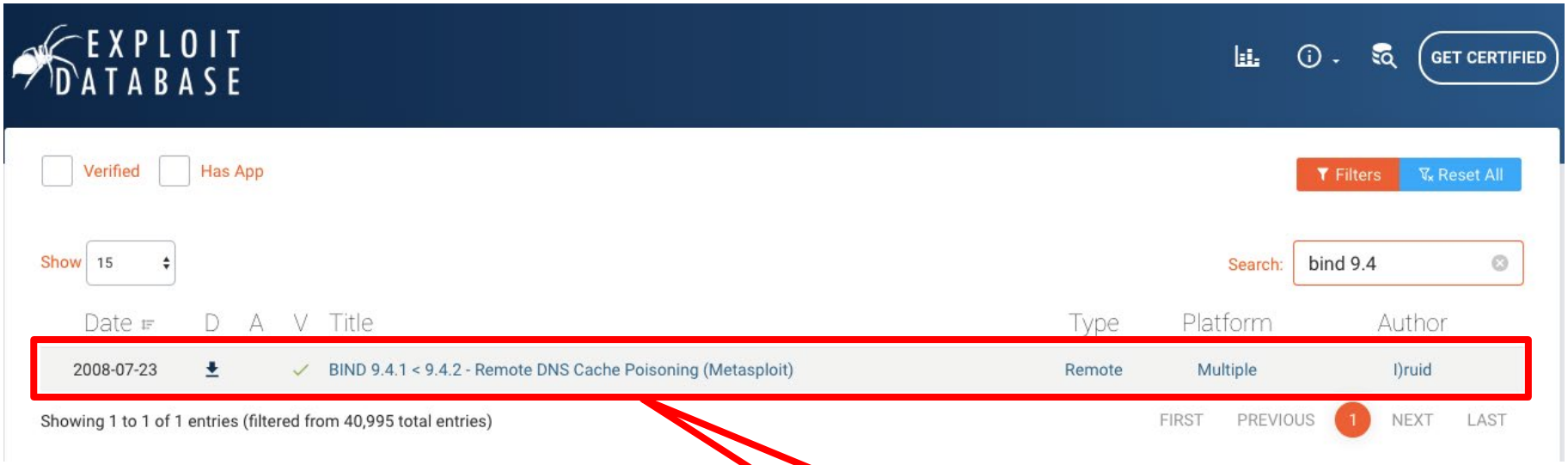


Analisi Manuale delle Vulnerabilità
Esempio 2

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

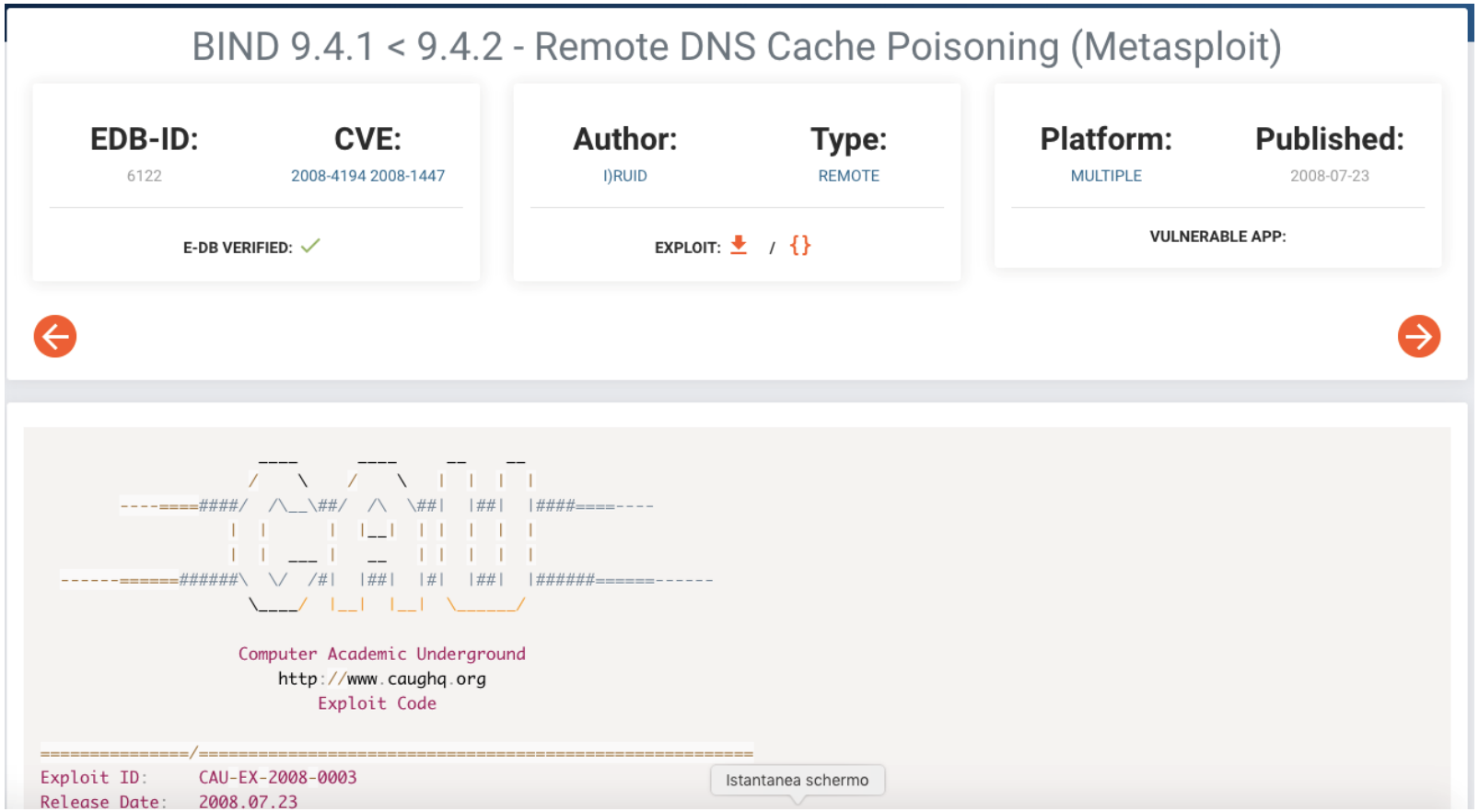


Analisi Manuale delle Vulnerabilità
Esempio 2



Risultato relativo alla versione del servizio cercato

Analisi Manuale delle Vulnerabilità
Esempio 2

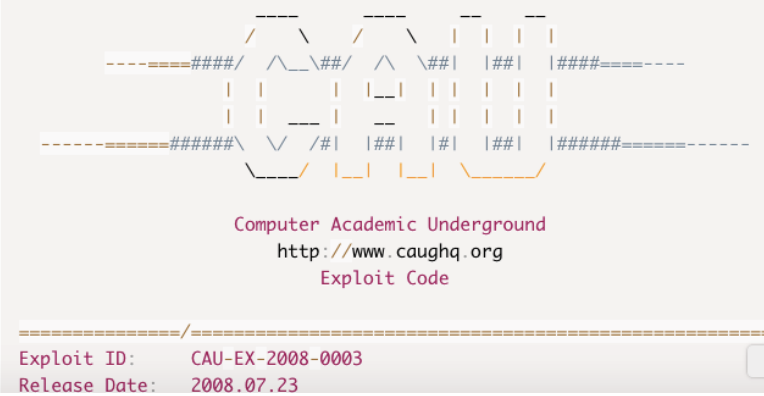


Analisi Manuale delle Vulnerabilità
Esempio 2

BIND 9.4.1 < 9.4.2 - Remote DNS Cache Poisoning (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Published:
6122	2008-4194 2008-1447	I)RUID	REMOTE	MULTIPLE	2008-07-23

E-DB VERIFIED: ✓ EXPLOIT: / {} VULNERABLE APP:



Potrei sfruttare questo exploit per effettuare un *Attacco di Pharming*