



Penetration Testing & Ethical Hacking

Vulnerability Mapping

Parte 2

Arcangelo Castiglione
arcastiglione@unisa.it

Caratterizzazione delle Vulnerabilità

National Vulnerability Database (NVD)

➤ <https://nvd.nist.gov/>

The screenshot shows the NIST NVD homepage. At the top, there's a navigation bar with the NIST logo, the "Information Technology Laboratory" link, and an "NVD MENU" button. Below the header, the "NATIONAL VULNERABILITY DATABASE" is prominently displayed. A yellow notice box titled "NOTICE UPDATE" contains the text: "NIST has updated the NVD program announcement page with additional information regarding recent concerns and the temporary delays in enrichment efforts." To the left, a sidebar lists links: General, Vulnerabilities, Vulnerability Metrics, Products, Developers, Contact NVD, Other Sites, and Search, each preceded by a plus sign. Below the sidebar are three circular icons: one showing a clipboard with binary code (labeled "New 2.0 APIs"), one showing a timeline with an arrow (labeled "Change Timeline"), and one showing a computer monitor displaying "KNOWN EXPLOITED VULNERABILITIES" (labeled "New Parameters").

- General
- Vulnerabilities
- Vulnerability Metrics
- Products
- Developers
- Contact NVD
- Other Sites
- Search

NOTICE UPDATE

NIST has updated the NVD program announcement page with additional information regarding recent concerns and the temporary delays in enrichment efforts.

New 2.0 APIs

Change Timeline

New Parameters

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics.

Caratterizzazione delle Vulnerabilità

National Vulnerability Database (NVD)

- Il National Vulnerability Database (**NVD**) è un archivio di informazioni **CVE** gestito dal National Institute of Standards and Technology (**NIST**)
 - **CVE** (Common Vulnerabilities and Exposures)
 - Maggiori dettagli successivamente...

- Costituisce una fonte molto completa di informazioni sulle vulnerabilità



Caratterizzazione delle Vulnerabilità

National Vulnerability Database (NVD)

- I punti chiave del **National Vulnerability Database (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 **National Vulnerability Database (NVD)** e per tutte le tassonomie delle vulnerabilità
- Maggiori dettagli in seguito...

The screenshot shows the NVD homepage with a blue header containing the NIST logo and the text "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE". On the right, there's a large "NVD" logo and a "CVSS" logo. The main content area has a sidebar with links like "General", "Vulnerabilities", "Vulnerability Metrics", "Products", "Configurations (CCE)", "Contact NVD", "Other Sites", and "Search". The main content area features a section titled "Vulnerability Metrics" with a detailed description of what CVSS is and how it's used. Below this is a section titled "Using CVSS support within NVD" with two numbered steps.

Vulnerability Metrics

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

The NVD supports both Common Vulnerability Scoring System (CVSS) v2.0 and v3.0 standards. The NVD provides CVSS 'base scores' which represent the innate characteristics of each vulnerability. We do not currently provide 'temporal scores' (metrics that change over time due to events external to the vulnerability) or 'environmental scores' (scores customized to reflect the impact of the vulnerability on your organization). However, the NVD does provide a CVSS score calculator to allow you to add temporal and environmental score data. This calculator contains support for U.S. government agencies to customize vulnerability impact scores based on FIPS 199 system ratings.

Using CVSS support within NVD

1. [NVD CVSS v3 Calculator](#) or [NVD CVSS v2 Calculator](#)
2. Click on a CVSS score while viewing a vulnerability detail page to customize that score using temporal and environmental metrics.

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

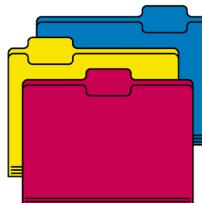
Outline

- 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

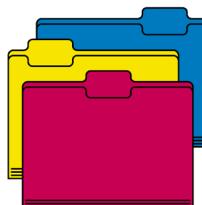
- Tuttavia
 - Nessuna tassonomia contiene una lista esaustiva di tutte le vulnerabilità che possono impattare sulla sicurezza di un asset
 - Una singola vulnerabilità potrebbe rientrare in più tassonomie



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 - Common Vulnerabilities and Exposure**
- Il **CVE (Common Vulnerabilities and Exposures)** 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/>

Search CVE List **Downloads** Data Feeds Update a CVE Record Request CVE IDs

TOTAL CVE Records: 277908

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and [CVE Record Format JSON](#) are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.
New CVE List download format is available now on [CVE.ORG](#).



mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Become a CNA

[CVE Numbering Authorities](#), or "CNAs," are essential to the CVE Program's success and every [CVE Record](#) is added to the [CVE List](#) by a CNA.

Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)

[Go to new CVE website](#)



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>

The screenshot shows the GitHub repository page for 'cvelistV5'. At the top, there are navigation links for 'main' (selected), '2 Branches', '20610 Tags', a search bar with 'Go to file', and a 'Code' button. Below this is a list of commits:

Commit	Message	Time Ago
cvelistV5 Github Action	9 changes (0 new 9 updated):	26c6886 · 9 minutes ago
.github/workflows	update all github actions to use specific commits, and cleanin...	2 months ago
cves	9 changes (0 new 9 updated):	9 minutes ago
.gitattributes	initial commit for "bulk download" task	2 years ago
.gitignore	improved log; only update recent_activities when there are n...	2 years ago
README.md	Update README.md	6 hours ago

Below the commits is the 'README' section, which contains a note about maintenance:

Note 2025-04-02 CVE Services Maintenance April 2 beginning at approximately 1:00 PM (until approximately 5:00 PM EDT): The CVE Program will be performing maintenance on CVE Services on April 2 between 1 and 5 PM EDT. This maintenance action will have no impact on existing CVE Records in the CVE List. Although the CVE Repository will be available during this time, it will not be updated with any newly published records until the maintenance is complete.

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

➤ <https://github.com/CVEProject/cvelistV5>

The screenshot shows the GitHub repository page for 'cvelistV5'. At the top, there are navigation links for 'main' (with a dropdown), '2 Branches', '20610 Tags', a search bar labeled 'Go to file', and a green 'Code' button. Below this is a list of commits:

Commit	Message	Time Ago
cvelistV5 Github Action	9 changes (0 new 9 updated):	26c6886 · 9 minutes ago
.github/workflows	update all github actions to use specific commits, and cleanin...	2 months ago
cves	9 changes (0 new 9 updated):	9 minutes ago
.gitattributes	initial commit for "bulk download" task	2 years ago
.gitignore	improved log: only update recent_activities when there are n...	2 years ago
README.md	Update README.md	6 hours ago

A red arrow points to the 'cves' commit. Below the commit list is the 'README' section, which contains the text: 'Lista dei CVE dal 1999 ad oggi'. At the bottom of the README, there is a note about maintenance: 'Note 2025-04-02 CVE Services Maintenance April 2 beginning at approximately 1:00 PM (until approximately 5:00 PM EDT): The CVE Program will be performing maintenance on CVE Services on April 2 between 1 and 5 PM EDT. This maintenance action will have no impact on existing CVE Records in the CVE List. Although the CVE Repository will be available during this time, it will not be updated with any newly published records until the maintenance is complete.'

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE)

➤ <https://cve.mitre.org/>

[Search CVE List](#) [Downloads](#) [Data Feeds](#) [Update a CVE Record](#) [Request CVE IDs](#)

TOTAL CVE Records: 277908

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and [CVE Record Format JSON](#) are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.
New CVE List download format is available now on [CVE.ORG](#).

mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Become a CNA

[CVE Numbering Authorities](#), or "CNAs," are essential to the CVE Program's success and every [CVE Record](#) is added to the [CVE List](#) by a CNA.

Join today!

- [Business benefits](#)
- [No fee or contract](#)
- [Few requirements](#)
- [Easy to join](#)

[Go to new CVE website](#)



Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

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



Search CVE List

You can search the CVE List for a [CVE Record](#) if the CVE

Attention: CVE Records now include product versions &

Ubuntu 18.10

Submit

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 obtain a user namespace.
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu1 uses 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 enabled, allows local users to gain root privileges by loading arbitrary kernel modules. This occurs because a modified kernel/module.c file is loaded without verification.

SEARCH CVE USING KEYWORD
You can also search by reference number
[For More Information](#)

Tassonomie CVE relative ad Ubuntu 18.10

Vulnerability Mapping

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 obtain a user namespace.
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu1 uses 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 enabled, allows local users to gain root privileges by loading arbitrary kernel modules. This occurs because a modified kernel/module.c file is used for verification.

SEARCH CVE USING KEYWORD
You can also search by reference number
[For More Information](#)

CVE-2018-6557 (MOTD = Message Of The Day)

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

Ubuntu

Product

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>

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an [OVAL query](#).

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type <input checked="" type="radio"/> Basic <input type="radio"/> Advanced	Contains HyperLinks <input type="checkbox"/> CISA Known Exploited Vulnerabilities <input type="checkbox"/> US-CERT Technical Alerts <input type="checkbox"/> US-CERT Vulnerability Notes <input type="checkbox"/> OVAL Queries
Results Type <input checked="" type="radio"/> Overview <input type="radio"/> Statistics	Contains Tags <input type="checkbox"/> Disputed <input type="checkbox"/> Unsupported When Assigned <input type="checkbox"/> Exclusively Hosted Service
Keyword Search <input type="text"/> <input type="checkbox"/> Exact Match	Search Reset
Search Type <input checked="" type="radio"/> All Time <input type="radio"/> Last 3 Months	

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>

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately by distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

The screenshot shows the 'Search Vulnerability Database' page. A red box highlights the search input field containing 'CVE-2018-6557'. A red arrow points from the text 'Ricerca di dettagli relativi al CVE-2018-6557 sul National Vulnerability Database (NVD)' to this input field. The page includes sections for 'Search Type' (Basic selected), 'Results Type' (Overview selected), 'Contains HyperLinks' (checkboxes for CISA Known Exploited Vulnerabilities and US-CERT Technical Alerts), 'Contains Tags' (checkboxes for Disputed, Unsupported When Assigned, and Exclusively Hosted Service), and 'Exact Match' (checkbox). At the bottom are 'Search' and 'Reset' buttons.

Search Type

Basic Advanced

Results Type

Overview Statistics

Contains HyperLinks

CISA Known Exploited Vulnerabilities

US-CERT Technical Alerts

Contains Tags

Disputed

Unsupported When Assigned

Exclusively Hosted Service

Exact Match

Keyword Search

CVE-2018-6557

Search Type

All Time Last 3 Months

Search Reset

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.	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.

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.

QUICK INFO

CVE Dictionary Entry:
CVE-2018-6557

NVD Published Date:
08/21/2018

NVD Last Modified:
11/20/2024

Source:
Canonical Ltd.

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

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.

Description

The MOTD update script in the base-files package in Ubuntu 10.1ubuntu6 incorrectly handled temporary files. A local attacker could possibly escalate privileges if kernel symlink restrictions were

CVSS v3.1 Severity and Metrics:

Base Score: 7.0 HIGH

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

Impact Score: 5.9

Exploitability Score: 1.0

Attack Vector (AV): Local

Attack Complexity (AC): High

Privileges Required (PR): Low

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Metrics

CVSS Version 4.0

CVSS Version 3.x

NVD enrichment efforts reference publicly available information to assess the severity of the vulnerability. The information used to calculate the score and sources is also displayed.

CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: 7.0 HIGH

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

QUICK INFO

CVE Dictionary Entry:

CVE-2018-6557

NVD Published Date:

08/21/2018

NVD Last Modified:

11/20/2024

Source:

Canonical Ltd.

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



Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. Search results will be the best matches for your search words. View the [search tips](#).

MS08-067

Attention: CVE Records now include product versions & more details.

MS08-067

Submit

- **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 cancellation. "Server Service Vulnerability."

SEARCH CVE USING KEYWORDS:

You can also search by reference using the [CVE Reference Search](#)

For More Information: [CVE Request Web Form](#) (select 'Search by Reference')

[Contact Us](#) | [Terms of Use](#) | [Privacy Policy](#) | [Site Map](#) | [Search this site](#)

Use of the Common Vulnerabilities and Exposures (CVE®) List and the associated references from this website are subject to the [terms of use](#). Created by the [U.S. Cybersecurity & Infrastructure Security Agency](#) (CISA). Copyright © 1999–2019, [The MITRE Corporation](#). CVE and the CVE logo are registered trademarks of The MITRE Corporation.

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – Ricerca

CVE-2008-4250

PUBLISHED

 [View JSON](#) |  [User Guide](#)

[Collapse all](#)

Required CVE Record Information

CNA: Microsoft Corporation

-

Published: 2008-10-23 Updated: 2018-10-12

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."

Product Status

[Learn more](#)

Information not provided

References 19 Total

- [secunia.com: 32326](#)  third-party-advisory

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposure (CVE) – NVD

➤ <https://nvd.nist.gov/vuln/search>

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are not included in the search results. Linux distributions.

Search results will only be returned for data that is populated by NIST or from source of Acceptable Use Policy.

Search Type

Basic Advanced

Results Type

Overview Statistics

Keyword Search

Exact Match

Contains HyperLinks

CISA Known Exploited Vulnerabilities

US-CERT Technical Alerts

US-CERT Vulnerability Notes

Contains Tags

Disputed

Unsupported When Assigned

Exclusively Hosted Service

Search Type

All Time Last 3 Months

Search **Reset**



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."	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	Exploit Required
http://blogs.securiteam.com/index.php/archives/1150	Exploit Required
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

Tassonomia delle Vulnerabilità

Common Vulnerabilities and Exposures (CVE) – NVD

Weakness Enumeration

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

CWE: Common
Weakness
Enumeration

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/>

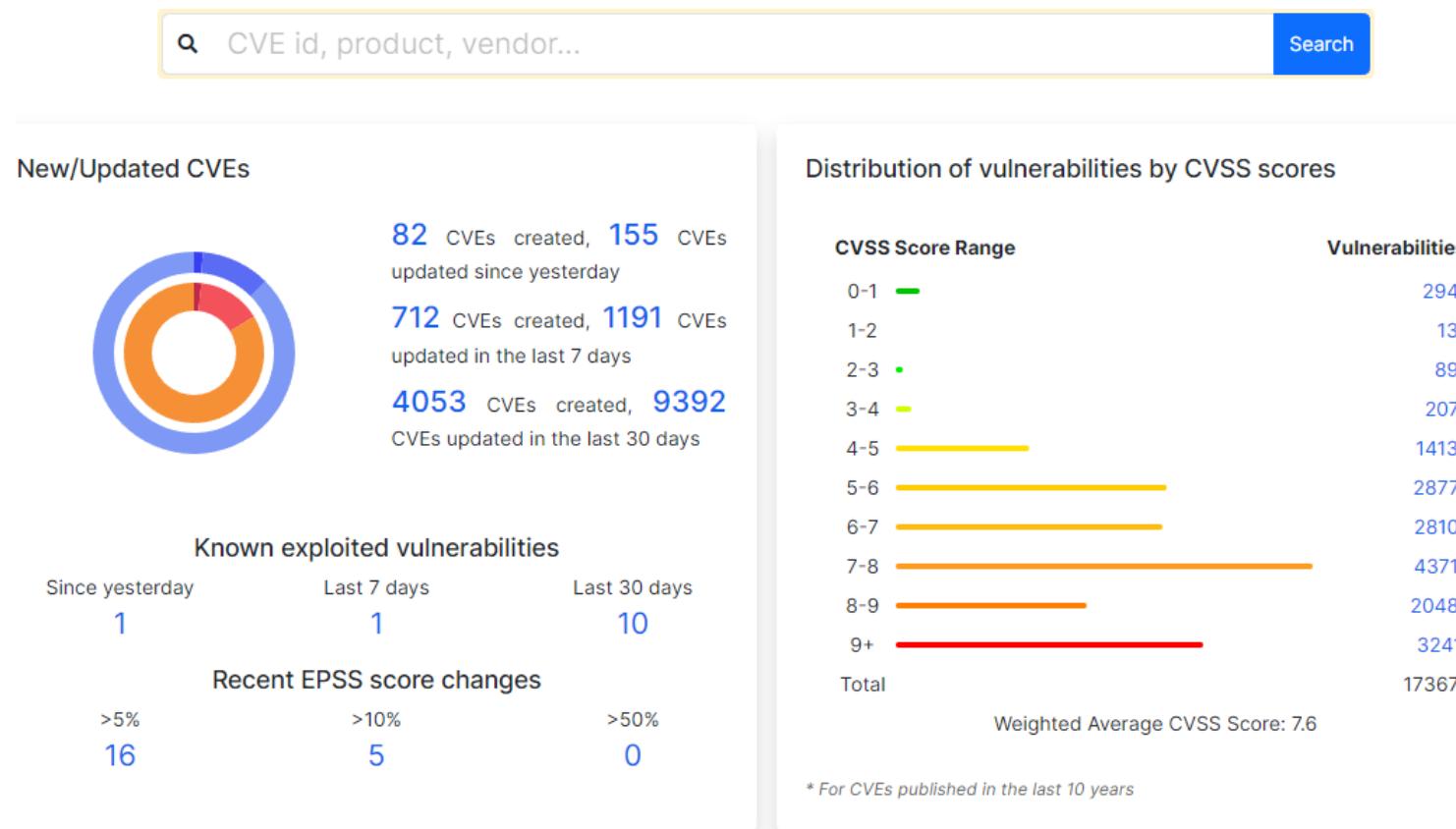
- Fornisce un'interfaccia Web facile da usare verso i dati CVE
- Permette di
 - Cercare **vulnerabilità relative ad aziende, prodotti, versioni di prodotti, etc**
 - Visualizzando le entry CVE correlate ad esse
 - Visualizzare **statistiche su aziende produttrici, prodotti e versioni dei prodotti, etc**
- 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

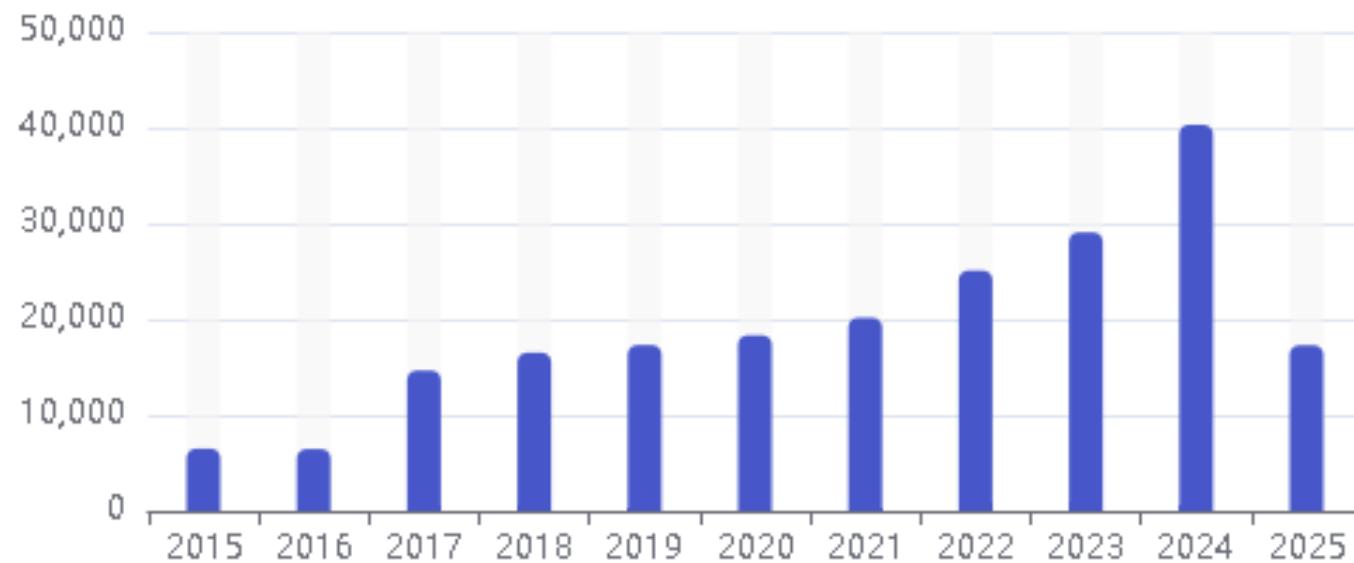
2025	17285	January	February	March	April	May							
2024	40301	January	February	March	April	May	June	July	August	September	October	November	December
2023	29066	January	February	March	April	May	June	July	August	September	October	November	December
2022	25084	January	February	March	April	May	June	July	August	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>

Number of CVEs by year



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>

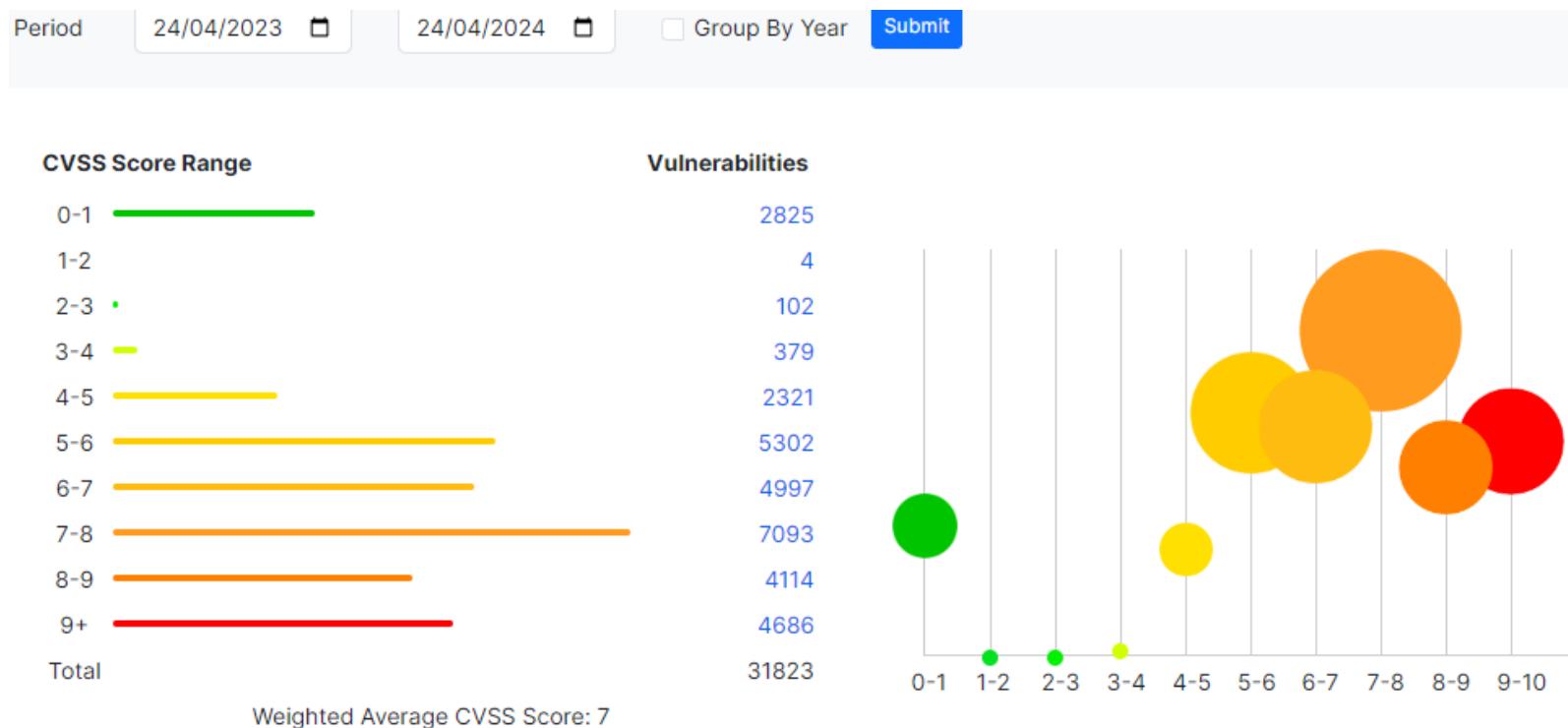
Vulnerabilities by impact types

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	<u>2024-04-22</u>	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>

 CVEdetails.com
powered by SecurityScorecard

✓ Vulnerabilities

-  By Date
-  By Type
-  Known Exploited

 Assigners

 CVSS Scores

 EPSS Scores

 Search

✓ Vulnerable Software

-  Vendors
-  Products
-  Version Search

Vendors - Vendor names starting with "A"



Vendor name, like apa* or ap*he

Search

Browse vendor names starting with:

 A                   

2488 vendors found



1

2

3

4

5

.....

47

48

49

50

▼ Vendor Name

[A M Kuchling](#)

[A Mennucc1](#)

[A-a-s Application Access Server](#)

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Vendor (Amazon)

➤ <https://www.cvedetails.com/vendor.php>

Vendor Search

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>

Vendor Search

Vendor Name	Number of Products	Number of Total Vulnerabilities
Apple	203	7205

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>

Vendor Search

<input type="text"/> dji	<input type="button" value="Search"/>	
Vendor Name	Number of Products	Number of Total Vulnerabilities
DJI	28	12

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>

Vendor Search

Vendor Name	Number of Products	Number of Total Vulnerabilities
-------------	--------------------	---------------------------------

Xiaomi	11	1
--------	----	---

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto

➤ <https://www.cvedetails.com/product-list.php>

 CVEdetails.com
powered by SecurityScorecard

▼ Vulnerabilities

-  By Date
-  By Type
-  Known Exploited
-  Assigners
-  CVSS Scores
-  EPSS Scores
-  Search

▼ Vulnerable Software

-  Vendors
-  Products
-  Version Search

List Of Products - Product name starting with "A"



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

Search

[Applications](#)

[Operating Systems](#)

[Hardware/Appliances](#)

All

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

9409 products found

>

1

2

3

4

5

.....

186

187

188

189

▼ Product Name

[A 220](#)

Me

[A 220 4matic](#)

Me

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Amazon Echo Dot)

➤ <https://www.cvedetails.com/product-list.php>

Product Search

Product Type: Application Operating System Hardware

#	Product Name	Vendor Name	Number of Vulnerabilities	Product Type	Risk Score
1	Echo Dot	Amazon	0	Hardware	
2	Echo Dot Firmware	Amazon	3	OS	

Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Raspberry)

➤ <https://www.cvedetails.com/product-list.php>

Product 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		Risk Score	◆ Vulnerabilities	◆ Product Type
Air 2			0	Hardware
Air 2 Firmware			1	OS
Air 2s			0	Hardware
Air 2s Firmware			1	OS
Phantom 4 Pro			0	Hardware
Phantom 4 Pro Firmware			1	OS
FPV			0	Hardware
Fpv Firmware			1	OS
Inspire 2			0	Hardware
Inspire 2 Firmware			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



Tassonomia delle Vulnerabilità

CVE Details – Ricerca per Prodotto (Huawei P40)

➤ <https://www.cvedetails.com/product-list.php>

Product 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	A
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>

Vendor, Product, Version Search

Vendor Name:

e.g Apache or apac*

Product Name:

e.g http*

Version:

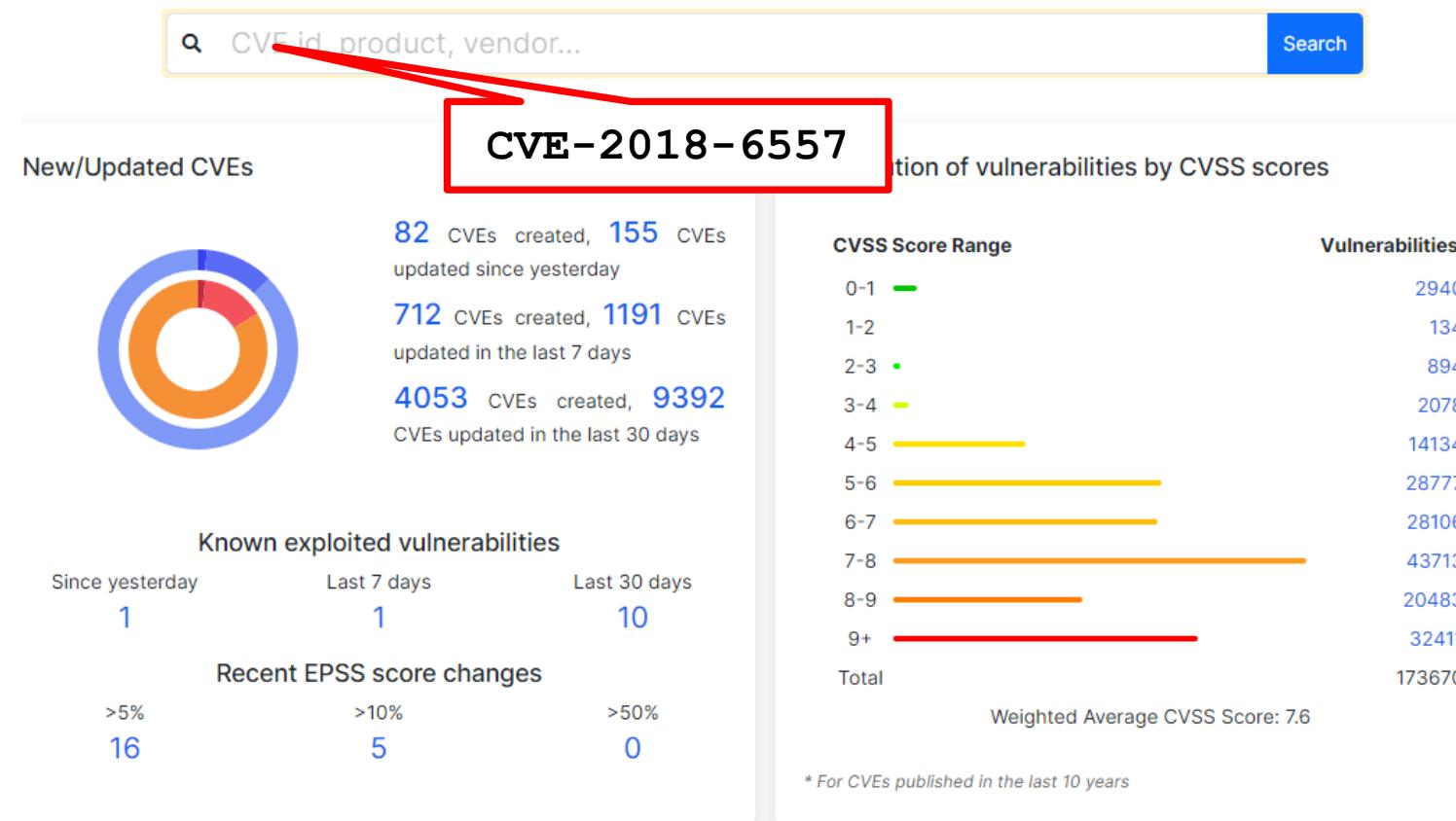
e.g 2.3* or 2.4.*

Search

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.](#)

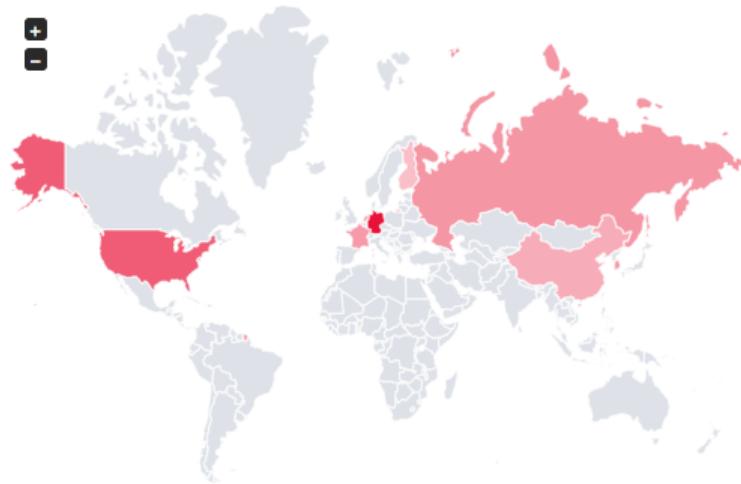
[View at NVD](#) [CVE.org](#)

Vulnerability category: Denial of service

Tassonomia delle Vulnerabilità

CVE Details – Esempio 1

Threat overview for CVE-2018-6557



Top 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 ↗](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 ↗](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/ ↗](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:***:*****:*

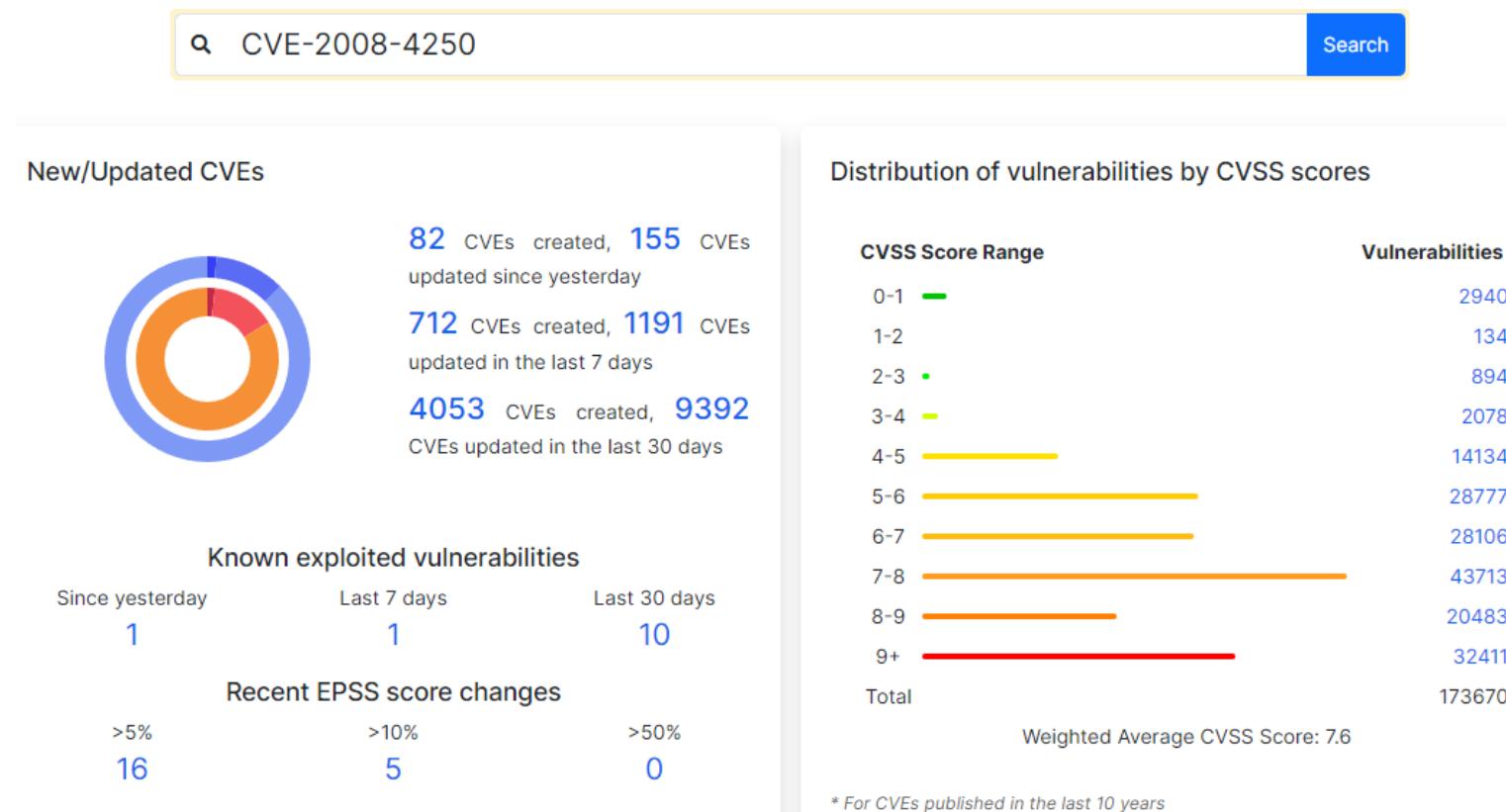
[Matching versions](#)

Tassonomia delle Vulnerabilità

CVE Details – Esempio 2

➤ <https://www.cvedetails.com/>

Vulnerabilità MS08-067



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

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)

Exploit per la
vulnerabilità

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:-:1;*: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 Known Exploited Vulnerabilities (KEV) è un catalogo, gestito dal U.S. Cybersecurity and Infrastructure Security Agency (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



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 been 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>

Filters

What are you looking for?

Date Added (optional)

Sort by (optional)

Publish Date

Items per page (optional)

20

Tassonomia delle Vulnerabilità

KEV – Ricerca Produttori

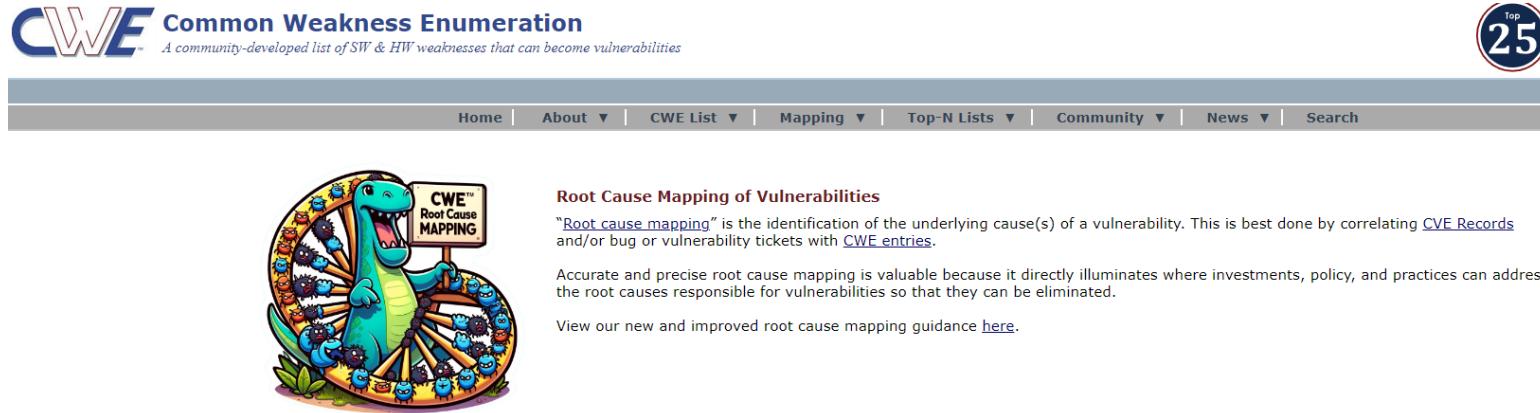
➤ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Vendor/Project	-
<input type="checkbox"/> Search...	
<input type="checkbox"/> Accellion	
<input type="checkbox"/> Qlik	
<input type="checkbox"/> Unitronics	
<input type="checkbox"/> FXC	
<input type="checkbox"/> Spreadsheet::ParseExcel	
<input type="checkbox"/> Joomla!	
<input type="checkbox"/> ConnectWise	
<input type="checkbox"/> Sunhill	
<input type="checkbox"/> Nice	
<input type="checkbox"/> ownCloud	
<input type="checkbox"/> Adobe	
<input type="checkbox"/> Alcatel	
<input type="checkbox"/> Amcrest	
<input type="checkbox"/> Android	
<input type="checkbox"/> Apache	

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
 - **Comprendere 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.



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



Welcome to the 2023 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses list (CWE™ Top 25). This list demonstrates the currently most common and impactful software weaknesses.

Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

[2023 Top 25 List](#) [Key Insights](#) [Methodology](#)



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: !\[\]\(9e9ae22e7d0a57826d353c2bd0c4711d_img.jpg\)](#) [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 underlying 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 Common Weakness Enumeration (CWE) ed al Common Vulnerabilities and Exposures (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/>



Understanding how the adversary operates is essential to effective cybersecurity. CAF understanding and enhance defenses.

A screenshot of the CAPEC List Quick Access page. It has a dark red header bar with the text "CAPEC List Quick Access". Below it is a search bar with the placeholder "Search CAPEC" and a note "ENHANCED BY Google". There is a "View CAPEC" button and three buttons for filtering: "by Mechanisms of Attack", "by Domains of Attack", and "by Other Criteria". At the bottom, it shows "Total Attack Patterns: 559".

Tassonomia delle Vulnerabilità

Common Attack Pattern Enumeration and Classification (CAPEC) – Interfaccia

➤ <https://capec.mitre.org/>

The screenshot shows the top navigation bar with links for Home, About, CAPEC List, Community, News, and Search. Below the navigation, a banner states: "CAPEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used to identify potential threats and to help in the development of security countermeasures." A yellow button on the left says "New to CAPEC? Start Here!" A section titled "New to CAPEC?" provides tips for newcomers. A red header bar at the bottom reads "Community Engagement".

PEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used to identify potential threats and to help in the development of security countermeasures.

New to CAPEC?

New to CAPEC?
Start Here!

Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.

Community Engagement

If you would like to be a part of ongoing discussions related to MITRE's work in shifting the balance of cybersecurity risk, please visit the [Common Weakness Enumeration \(CWE™\)](#) website.

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

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

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

- 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

- 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	Gain Privileges
Authorization	

<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>

CAPEC List Version 3.9

Total Attack Patterns: 559

[Latest Version](#) | [Downloads](#) | [Reports](#) | [Archive](#)

Latest Version

The Common Attack Pattern Enumeration and Classification (CAPEC™) effort provides a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy. The entire list of CAPEC entries developed to date is accessible below for review or download.

Navigate CAPEC

Use one of the hierarchical representations below to navigate the entire list according to your specific point of view. The Mechanisms of Attack representation organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The Domains of Attack representation organizes items by the target domains for each attack pattern.

[View by Mechanisms of Attack](#)

[View by Domains of Attack](#)

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

Tassonomia delle Vulnerabilità

Ricapitolazione: CVE, CWE, CAPEC ed NVD

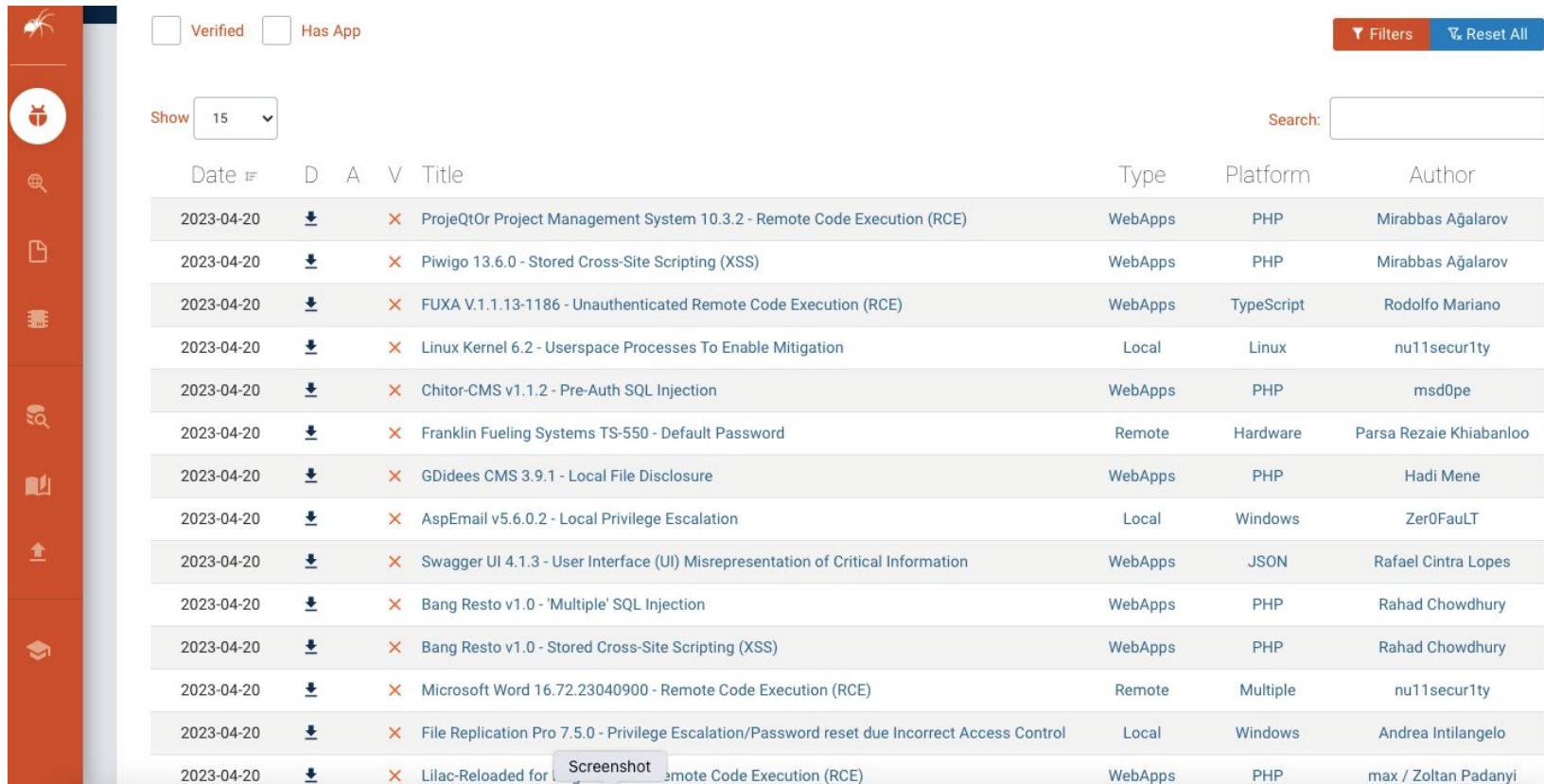
- **CVE, KEV, CWE, CAPEC ed NVD** sono componenti essenziali per la gestione delle vulnerabilità
 - **CVE** fornisce identificatori univoci per vulnerabilità specifiche
 - **KEV** fornisce indicazioni sulle vulnerabilità che sono state sfruttate
 - **CWE** classifica le debolezze comuni di software e 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/>

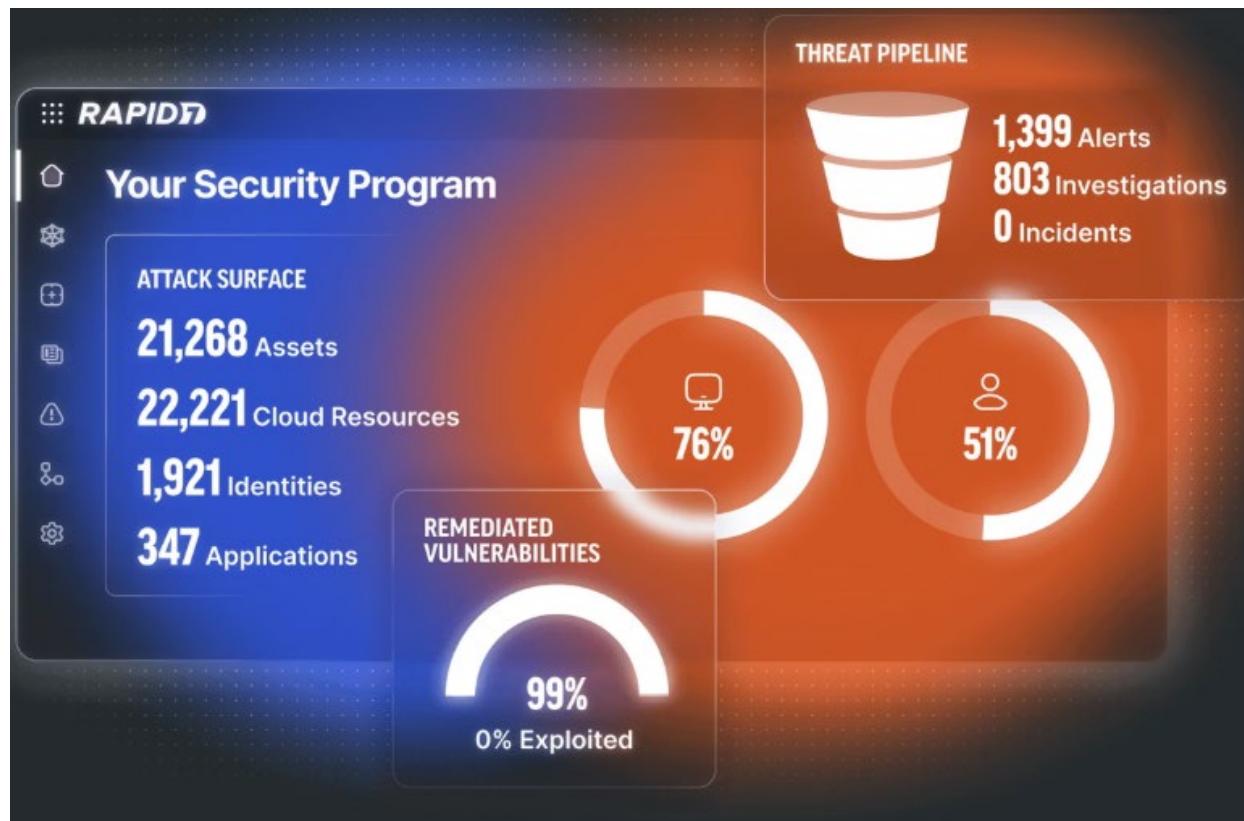


Date	D	A	V	Title	Type	Platform	Author
2023-04-20	↓	X		ProjeQtOr Project Management System 10.3.2 - Remote Code Execution (RCE)	WebApps	PHP	Mirabbas Ağalarov
2023-04-20	↓	X		Piwigo 13.6.0 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Mirabbas Ağalarov
2023-04-20	↓	X		FUXA V.1.1.13-1186 - Unauthenticated Remote Code Execution (RCE)	WebApps	TypeScript	Rodolfo Mariano
2023-04-20	↓	X		Linux Kernel 6.2 - Userspace Processes To Enable Mitigation	Local	Linux	nu11secur1ty
2023-04-20	↓	X		Chitor-CMS v1.1.2 - Pre-Auth SQL Injection	WebApps	PHP	msd0pe
2023-04-20	↓	X		Franklin Fueling Systems TS-550 - Default Password	Remote	Hardware	Parsa Rezaie Khiabanloo
2023-04-20	↓	X		GDidees CMS 3.9.1 - Local File Disclosure	WebApps	PHP	Hadi Mene
2023-04-20	↓	X		AspEmail v5.6.0.2 - Local Privilege Escalation	Local	Windows	Zer0FauLT
2023-04-20	↓	X		Swagger UI 4.1.3 - User Interface (UI) Misrepresentation of Critical Information	WebApps	JSON	Rafael Cintra Lopes
2023-04-20	↓	X		Bang Resto v1.0 - 'Multiple' SQL Injection	WebApps	PHP	Rahad Chowdhury
2023-04-20	↓	X		Bang Resto v1.0 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Rahad Chowdhury
2023-04-20	↓	X		Microsoft Word 16.72.23040900 - Remote Code Execution (RCE)	Remote	Multiple	nu11secur1ty
2023-04-20	↓	X		File Replication Pro 7.5.0 - Privilege Escalation/Password reset due Incorrect Access Control	Local	Windows	Andrea Intilangelo
2023-04-20	↓	X		Lilac-Reloaded for Screenshot Remote Code Execution (RCE)	WebApps	PHP	max / Zoltan Padanyi

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/>

» SECUNIA RESEARCH

Access authoritative security advisories from Secunia Research

Since 2002 the team at Secunia Research have been delivering security advisories that provide reliable, curated, actionable vulnerability intelligence. These security advisories provide a summary of the body of work that Secunia Research performs in order to communicate a standardized, validated, and enriched vulnerability research on a specific version of a software product.

Contact us → Watch video (0:29) ◎

RELATED

- Secunia Research
- Secunia Research disclosure policy
- Software Vulnerability Research
- Software Vulnerability Manager
- Report a vulnerability

Tassonomia delle Vulnerabilità

Altre Fonti – Core Security

➤ <https://www.coresecurity.com/products/core-impact/recent-exploits-and-updates>

The screenshot shows the top navigation bar of the Core Security website. It includes links for "Contact Us", "Support", and several dropdown menus labeled "CYBER THREAT", "IDENTITY", "INDUSTRIES", and "RESOURCES".

Exploit Name Vulnerability Platform [- Any -] Exploit Type Product Name

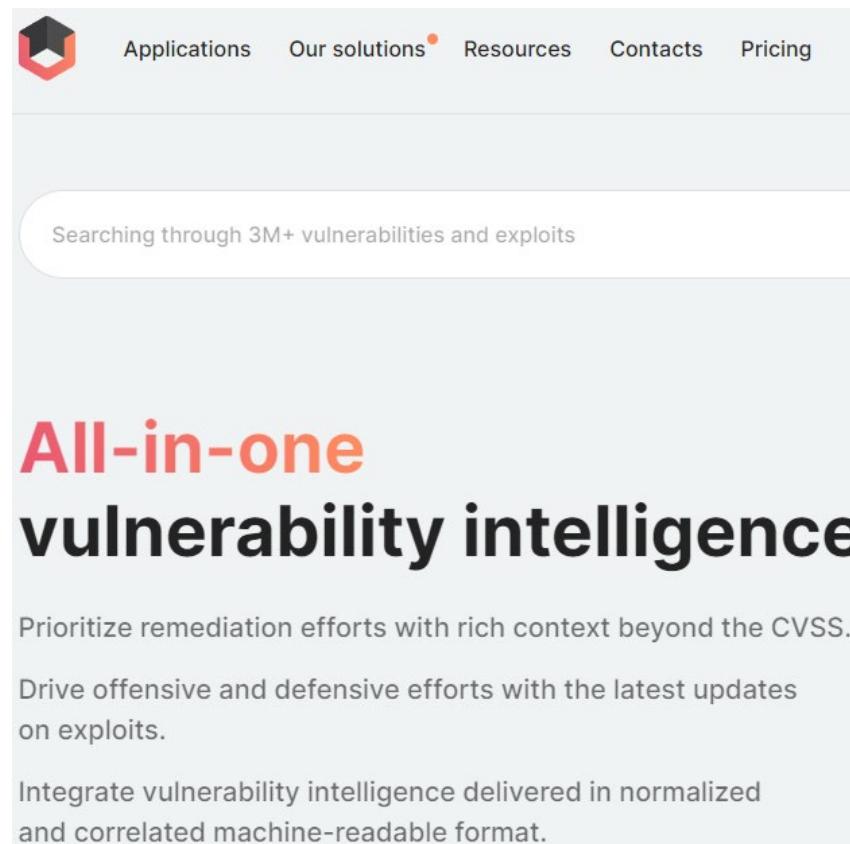
Title	Description	Date Added	CVE Link	Exploit Platform	Exploit Type	Product Name
Veeam Backup and Replication Backup Service Remote Code Execution Exploit	A vulnerability in the Backup Service of Veeam Backup and Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts. This update adds a module that checks the vulnerability and retrieves all the credentials and another module to deploy an agent.	April 21, 2023	CVE-2023-27532	Windows	Exploits / Remote Code Execution	Impact
VMware vRealize Log Insight Multiple Vulnerabilities Remote Code Execution Exploit	This module exploits an information disclosure vulnerability, a remote file download vulnerability and a directory traversal vulnerability in VMware vRealize Log Insight to deploy an agent with root privileges.	April 11, 2023	CVE-2022-31711	Linux	Exploits / Remote Code Execution	Impact



Tassonomia delle Vulnerabilità

Altre Fonti – Vulners

➤ <https://vulners.com/>



Tassonomia delle Vulnerabilità

Altre Fonti – Vulners – Esempio

The screenshot shows the Vulners search interface. A red arrow points from the search bar to the search result 'ms08-067'. The result is highlighted with a red box. Below the search bar, there are several navigation links: Daily Hot!, Security news, Exploit updates, Blogs review, Linux vulnerabilities, Bugbounty, AI High Score, and CVE Feed. Underneath these are filters for CVSS High Score, EPSS High Score, Wild exploited, and a 'show all' link. The main result card for 'ms08-067' features the NSA/CISA logo and the title 'NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations'. It includes a summary: 'A plea for network defenders and software manufacturers to fix common problems. EXECUTIVE SUMMARY The National Security Agency (NSA) and C...'. Below the summary are metrics: CVSS 10, AI Score 10, EPSS 0.976, and a publish date of 2023-10-05 12:00 PM. There are 36 comments.

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 **Exploit DataBase (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

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x + ▾
root@kali:~# nmap -sV -T5 -p- 10.0.2.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-15 17:45 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0032s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      openSSH 4.7/p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs     2-4 (RPC #100003)
2121/tcp  open  ftp     ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

Analisi Manuale delle Vulnerabilità

Esempio 1

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

The screenshot shows the Exploit Database homepage. On the left is a vertical sidebar with orange icons for various tools: Spiders (Exploit), Bug (Has App), Magnifying Glass (Search), Document (PDF), Book (Bundles), Magnifying Glass (Search), Book (Bundles), Up Arrow (Upload), Hat (PWK), and WiFi (WIFU). The main area has a dark blue header with the 'EXPLOIT DATABASE' logo. Below the header is a search bar with filters for 'Verified' and 'Has App'. A red box highlights the search term 'vsftpd 2.3.4' in the search input field. The results table shows 15 entries from March 15, 2019. One entry for 'vsftpd 2.3.4' is highlighted with a red box and a red arrow pointing to it. The table includes columns for Date, Type, Title, Author, and various metadata.

Date	Type	Title	Author
2019-03-15	WebApps	Moodle 3.4.1 - Remote Code Execution	Darryn Ten
2019-03-15	WebApps	Laundry CMS - Multiple Vulnerabilities	Mehmet EMIROGLU
2019-03-15	WebApps	Vembu Storegrid Web Interface 4.4.0 - Multiple Vulnerabilities	Gionathan Reale
2019-03-15	WebApps	ICE HRM 23.0 - Multiple Vulnerabilities	Mehmet EMIROGLU
2019-03-15	Remote	Mail Carrier 2.5.1 - 'MAIL FROM' Buffer Overflow	Joseph McDonagh
2019-03-15	WebApps	CMS Made Simple Showtime2 Module 3.6.2 - Authenticated Arbitrary File Upload	Daniele Scana
2019-03-15	WebApps	NetData 1.13.0 - HTML Injection	s4vitar
2019-03-14	Remote	Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution	sud0woodo
2019-03-14	Remote	FTPGetter Standard 5.97.0.177 - Remote Code Execution	w4fz5uck5
2019-03-14	WebApps	Pegasus CMS 1.0 - 'extra_fields.php' Plugin Remote Code Execution	R3zk0n
2019-03-14	WebApps	Intel Modular Server System 10.18 - Cross-Site Request Forgery (Change Admin Password)	LiquidWorm

Analisi Manuale delle Vulnerabilità

Esempio 1

The screenshot shows a web-based search interface for vulnerabilities. At the top, there are two unchecked checkboxes: "Verified" and "Has App". To the right are buttons for "Filters" and "Reset All". Below this, a search bar contains the text "vsftpd 2.3.4" with a clear button. A "Show" dropdown is set to 15 entries. The main table has columns for Date, Type, Platform, and Author. A single row is highlighted with a red border, corresponding to the search term. The row details a vulnerability found on 2011-07-05, categorized as Remote for Unix, and attributed to Metasploit. The title of the vulnerability is "vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)". At the bottom, a message states "Showing 1 to 1 of 1 entries (filtered from 40,995 total entries)" and includes navigation links for FIRST, PREVIOUS, NEXT (with a red circle containing the number 1), and LAST.

Date	Type	Platform	Author
2011-07-05	Remote	Unix	Metasploit

Risultato relativo alla
versione del servizio cercato

Analisi Manuale delle Vulnerabilità

Esempio 1

The screenshot shows a web-based search interface for vulnerabilities. At the top, there are two unchecked checkboxes: "Verified" and "Has App". On the right, there are buttons for "Filters" and "Reset All". Below this, there are search fields: "Show" set to 15, a date range from "2011-07-05" to "2011-07-05", and a search bar containing "vsftpd 2.3.4". A red arrow points to the search result row.

Date	Type	Platform	Author
2011-07-05	Remote	Unix	Metasploit

Showing 1 to 1 of 1 entries (filtered from 40,995 total entries)

Seleziono il risultato trovato

Analisi Manuale delle Vulnerabilità

Esempio 1

vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

EDB-ID:	17491	CVE:		Author:	METASPLOIT	Type:	REMOTE	Platform:	UNIX	Published:	2011-07-05
E-DB VERIFIED: ✓				EXPLOIT: Download / Source				VULNERABLE APP: Check			

\$Id: vsftpd_234_backdoor.rb 13099 2011-07-05 05:20:47Z hdm \$

This file is part of the Metasploit Framework and may be subject to
redistribution and commercial restrictions. Please see the Metasploit
Framework web site for more information on licensing and terms of use.
http://metasploit.com/framework/

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
Rank = ExcellentRanking

Istantanea schermo

Analisi Manuale delle Vulnerabilità

Esempio 1 (Approccio Alternativo)

Cerco su Google: **vsftpd 2.3.4** seguito dalla parola **exploit**

vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) - Exploit-DB
<https://www.exploit-db.com/exploits/17491> ▾ Traduci questa pagina

5 lug 2011 - This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent ...

Analisi Manuale delle Vulnerabilità

Esempio 2

```
root@kali:~# nmap -sV -T5 -p- 10.0.2.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-15 17:45 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0032s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntul (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtnd bind 9.4.2
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

Analisi Manuale delle Vulnerabilità

Esempio 2

➤ <https://www.exploit-db.com/>

The screenshot shows the Exploit Database homepage. On the left is a vertical sidebar with orange icons for various tools: Spider (ExploitDB), Bug (ExploitDB), Magnifying Glass (Search), Document (PDF), Book (Documentation), Magnifying Glass (Search), Book (Documentation), Up Arrow (Upload), Hat (PWK), and WiFi (WIFU). The main content area has a dark blue header with the 'EXPLOIT DATABASE' logo. Below the header is a search bar with filters for 'Verified' and 'Has App', and buttons for 'Filters' and 'Reset All'. The main table lists vulnerabilities with columns for Date, Title, Type, Platform, and Author. One specific entry for 'bind 9.4' is highlighted with a red box and a red arrow pointing to it.

Date	Title	Type	Platform	Author
2019-03-15	Moodle 3.4.1 - Remote Code Execution			Darryn Ten
2019-03-15	Laundry CMS - Multiple Vulnerabilities			Mehmet EMIROGLU
2019-03-15	Vembu Storegrid Web Interface 4.4.0 - Multiple Vulnerabilities	WebApps	PHP	Gionathan Reale
2019-03-15	ICE HRM 23.0 - Multiple Vulnerabilities	WebApps	PHP	Mehmet EMIROGLU
2019-03-15	Mail Carrier 2.5.1 - 'MAIL FROM' Buffer Overflow	Remote	Windows	Joseph McDonagh
2019-03-15	CMS Made Simple Showtime2 Module 3.6.2 - Authenticated Arbitrary File Upload	WebApps	PHP	Daniele Scana
2019-03-15	NetData 1.13.0 - HTML Injection	WebApps	Multiple	s4vitar
2019-03-14	Apache UNO / LibreOffice Version: 6.1.2 / OpenOffice 4.1.6 API - Remote Code Execution	Remote	Multiple	sud0woodo
2019-03-14	FTPGetter Standard 5.97.0.177 - Remote Code Execution	Remote	Windows	w4fz5uck5
2019-03-14	Pegasus CMS 1.0 - 'extra_fields.php' Plugin Remote Code Execution	WebApps	PHP	R3zk0n
2019-03-14	Intel Modular Server System 10.18 - Cross-Site Request Forgery (Change Admin Password)	WebApps	PHP	LiquidWorm

Analisi Manuale delle Vulnerabilità

Esempio 2

The screenshot shows the Exploit Database search results for the query "bind 9.4". A single result is highlighted with a red border:

Date	Type	Platform	Author
2008-07-23	Remote	Multiple	l)ruid

A red callout box points to the result row with the text: "Risultato relativo alla versione del servizio cercato".

Showing 1 to 1 of 1 entries (filtered from 40,995 total entries)

FIRST PREVIOUS 1 NEXT LAST

Analisi Manuale delle Vulnerabilità

Esempio 2

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

EDB-ID: 6122	CVE: 2008-4194 2008-1447	Author: I)RUID	Type: REMOTE	Platform: MULTIPLE	Published: 2008-07-23
E-DB VERIFIED: ✓		EXPLOIT: / {}		VULNERABLE APP:	

← →

Computer Academic Underground
<http://www.caughq.org>
Exploit Code

Exploit ID: CAU-EX-2008-0003
Release Date: 2008.07.23

Istantanea schermo

Analisi Manuale delle Vulnerabilità

Esempio 2

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

EDB-ID:

6122

CVE:

2008-4194 2008-1447

Author:

I)RUID

Type:

REMOTE

Platform:

MULTIPLE

Published:

2008-07-23

E-DB VERIFIED: ✓

EXPLOIT: ↴ / { }

VULNERABLE APP:



Computer Academic Underground
<http://www.caughq.org>
Exploit Code

Exploit ID: CAU-EX-2008-0003
Release Date: 2008.07.23

Istantanea schermo

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