Elenco CVE con peso

I risultati grezzi di ogni scansione sono salvati all'interno della directory
/home/ubuntu/Desktop/progetto/Docklz/results/8-6-2024__10-53-25

Ecco i 89 CVE a cui è potenzialmente vulnerabile l'immagine analizzata, ordinati in ordine decrescente di peso [max=3, min=0], un parametro calcolato che stima la rilevanza del CVE

```
-------------------
VulnerabilityID: CVE-2016-2781
Title: coreutils: Non-privileged session can escape to the parent session in chroot
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-33599
Title: glibc: stack-based buffer overflow in netgroup cache
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2016-20013
Title:
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-33599
Title: glibc: stack-based buffer overflow in netgroup cache
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2016-20013
Title:
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-40735
Title:
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-4899
Title: zstd: mysql: buffer overrun in util.c
Peso: 2 - Monitorare e pianificare l'intervento
```

```
-------------------
VulnerabilityID: CVE-2024-33599
Title: glibc: stack-based buffer overflow in netgroup cache
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2016-20013
Title:
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-40735
Title:
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-40152
Title: woodstox-core: woodstox to serialise XML data was vulnerable to Denial of Service attacks
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2023-1370
Title: json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2023-33202
Title: bc-java: Out of memory while parsing ASN.1 crafted data in org.bouncycastle.openssl.PEMParser class
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2024-1597
Title: pgjdbc: PostgreSQL JDBC Driver allows attacker to inject SQL if using PreferQueryMode=SIMPLE
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27943
Title: binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
```

```
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33600
Title: glibc: null pointer dereferences after failed netgroup cache insertion
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33601
Title: glibc: netgroup cache may terminate daemon on memory allocation failure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33602
Title: glibc: netgroup cache assumes NSS callback uses in-buffer strings
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33600
Title: glibc: null pointer dereferences after failed netgroup cache insertion
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33601
Title: glibc: netgroup cache may terminate daemon on memory allocation failure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33602
Title: glibc: netgroup cache assumes NSS callback uses in-buffer strings
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27943
Title: binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-2236
Title: libgcrypt: vulnerable to Marvin Attack
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26458
Title: krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2024-26461
Title: krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26458
Title: krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26461
Title: krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26458
Title: krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26461
Title: krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26458
Title: krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-26461
Title: krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-22916
Title: Denial of service via decompression of crafted file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-50495
Title: ncurses: segmentation fault via _nc_wrap_entry()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-50495
Title: ncurses: segmentation fault via _nc_wrap_entry()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-11164
Title: pcre: OP_KETRMAX feature in the match function in pcre_exec.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3857
Title: libpng: Null pointer dereference leads to segmentation fault
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-2511
Title: openssl: Unbounded memory growth with session handling in TLSv1.3
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-4603
```

```
Title: openssl: Excessive time spent checking DSA keys and parameters
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-4741
Title: openssl: Use After Free with SSL_free_buffers
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27943
Title: binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-7008
Title: systemd-resolved: Unsigned name response in signed zone is not refused when DNSSEC=yes
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-50495
Title: ncurses: segmentation fault via _nc_wrap_entry()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-7008
Title: systemd-resolved: Unsigned name response in signed zone is not refused when DNSSEC=yes
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33600
Title: glibc: null pointer dereferences after failed netgroup cache insertion
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33601
Title: glibc: netgroup cache may terminate daemon on memory allocation failure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-33602
Title: glibc: netgroup cache assumes NSS callback uses in-buffer strings
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-29383
Title: shadow: Improper input validation in shadow-utils package utility chfn
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-50495
Title: ncurses: segmentation fault via _nc_wrap_entry()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-50495
Title: ncurses: segmentation fault via _nc_wrap_entry()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-2511
Title: openssl: Unbounded memory growth with session handling in TLSv1.3
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-4603
Title: openssl: Excessive time spent checking DSA keys and parameters
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2024-4741
Title: openssl: Use After Free with SSL_free_buffers
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-29383
Title: shadow: Improper input validation in shadow-utils package utility chfn
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-31879
Title: wget: authorization header disclosure on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-29025
Title: netty-codec-http: Allocation of Resources Without Limits or Throttling
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-29025
Title: netty-codec-http: Allocation of Resources Without Limits or Throttling
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-44483
Title: santuario: Private Key disclosure in debug-log output
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-44483
Title: santuario: Private Key disclosure in debug-log output
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-15522
Title: bouncycastle: Timing issue within the EC math library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-45146
Title: bouncy-castle: Improper Authentication
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-15522
Title: bouncycastle: Timing issue within the EC math library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-33201
Title: bouncycastle: potential  blind LDAP injection attack using a self-signed certificate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-30171
Title: bc-java: BouncyCastle vulnerable to a timing variant of Bleichenbacher (Marvin Attack)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-23449
Title: elasticsearch: uncaught exception leads to crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-23450
```

```
Title: elasticsearch: Possible denial of service when processing documents in a deeply nested pipeline
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2024-23451
Title: elasticsearch: Incorrect authorization issue in Remote Cluster Security
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2023-45918
Title: ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinf ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2023-45918
Title: ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinf ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2023-45918
Title: ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinf ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2023-45918
Title: ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinf ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2023-45918
Title: ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinf ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2023-52428
Title: Denial of Service in Connect2id Nimbus JOSE+JWT
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2024-29857
Title: An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castl ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2024-29857
Title: An issue was discovered in ECCurve.java and ECCurve.cs in Bouncy Castl ...
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2024-30172
Title: An issue was discovered in Bouncy Castle Java Cryptography APIs before ...
Peso: 0 - Situazione sotto controllo
-------------------
```