Elenco CVE con peso

I risultati grezzi di ogni scansione sono salvati all'interno della directory
/home/ubuntu/Desktop/progetto/Docklz/results/7-6-2024__0-16-54

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-2017-13716
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-13716
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-13716
```

```
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2016-2781
Title: coreutils: Non-privileged session can escape to the parent session in chroot
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-2022-27943
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-2022-3219
Title: gnupg: denial of service issue (resource consumption) using compressed packets
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-13716
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2016-20013
Title:
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2016-20013
Title:
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-13716
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-13716
Title: binutils: Memory leak with the C++ symbol demangler routine in libiberty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20657
Title: libiberty: Memory leak in demangle_template function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1010204
Title: binutils: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read in gold/fileread.cc and
elfcpp/elfcpp_file.h leads to denial of service
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-2022-48064
Title: binutils: excessive memory consumption in _bfd_dwarf2_find_nearest_line_with_alt() in dwarf2.c
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-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.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-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.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-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.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-2024-26462
Title: krb5: Memory leak at /krb5/src/kdc/ndr.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-2022-40735
Title:
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-2022-4899
Title: zstd: mysql: buffer overrun in util.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2016-20013
Title:
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-2022-40735
Title: 
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-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
-------------------
```