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__11-1-46

L'immagine analizzata è risultata potenzialmente vulenrabile a 950 CVE. Vengono ordinati in ordine decrescente di peso [max=3, min=0], un parametro calcolato che stima la rilevanza del CVE

```
-------------------
VulnerabilityID: CVE-2020-1745
Title: undertow: AJP File Read/Inclusion Vulnerability
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-1938
Title: tomcat: Apache Tomcat AJP File Read/Inclusion Vulnerability
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-12900
Title: bzip2: out-of-bounds write in function BZ2_decompress
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-0500
Title: curl: Heap-based buffer overflow in Curl_smtp_escape_eob() when uploading data over SMTP
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000300
Title: curl: FTP shutdown response heap-based buffer overflow can potentially lead to RCE
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-14618
Title: curl: NTLM password overflow via integer overflow
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-5482
Title: curl: heap buffer overflow in function tftp_receive_packet()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-22945
Title: curl: use-after-free and double-free in MQTT sending
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-32207
Title: curl: Unpreserved file permissions
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-0500
Title: curl: Heap-based buffer overflow in Curl_smtp_escape_eob() when uploading data over SMTP
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000300
Title: curl: FTP shutdown response heap-based buffer overflow can potentially lead to RCE
Peso: 2 - Monitorare e pianificare l'intervento
```

```
-------------------
VulnerabilityID: CVE-2018-14618
Title: curl: NTLM password overflow via integer overflow
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16839
Title: curl: Integer overflow leading to heap-based buffer overflow in Curl_sasl_create_plain_message()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16840
Title: curl: Use-after-free when closing "easy" handle in Curl_close()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16842
Title: curl: Heap-based buffer over-read in the curl tool warning formatting
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3822
Title: curl: NTLMv2 type-3 header stack buffer overflow
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-5481
Title: curl: double free due to subsequent call of realloc()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-5482
Title: curl: heap buffer overflow in function tftp_receive_packet()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-22945
Title: curl: use-after-free and double-free in MQTT sending
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-32207
Title: curl: Unpreserved file permissions
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-0500
Title: curl: Heap-based buffer overflow in Curl_smtp_escape_eob() when uploading data over SMTP
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000300
Title: curl: FTP shutdown response heap-based buffer overflow can potentially lead to RCE
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000301
Title: curl: Out-of-bounds heap read when missing RTSP headers allows information leak or denial of service
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-14618
Title: curl: NTLM password overflow via integer overflow
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16839
```

```
Title: curl: Integer overflow leading to heap-based buffer overflow in Curl_sasl_create_plain_message()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16840
Title: curl: Use-after-free when closing "easy" handle in Curl_close()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16842
Title: curl: Heap-based buffer over-read in the curl tool warning formatting
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3822
Title: curl: NTLMv2 type-3 header stack buffer overflow
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-5481
Title: curl: double free due to subsequent call of realloc()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-5482
Title: curl: heap buffer overflow in function tftp_receive_packet()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-22945
Title: curl: use-after-free and double-free in MQTT sending
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-32207
Title: curl: Unpreserved file permissions
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16402
Title: elfutils: Double-free due to double decompression of sections in crafted ELF causes crash
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16402
Title: elfutils: Double-free due to double decompression of sections in crafted ELF causes crash
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22822
Title: expat: Integer overflow in addBinding in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22823
Title: expat: Integer overflow in build_model in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22824
Title: expat: Integer overflow in defineAttribute in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23852
Title: expat: Integer overflow in function XML_GetBuffer
Peso: 2 - Monitorare e pianificare l'intervento
```

```
-------------------
VulnerabilityID: CVE-2022-25235
Title: expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25236
Title: expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25315
Title: expat: Integer overflow in storeRawNames()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22822
Title: expat: Integer overflow in addBinding in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22823
Title: expat: Integer overflow in build_model in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22824
Title: expat: Integer overflow in defineAttribute in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23852
Title: expat: Integer overflow in function XML_GetBuffer
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25235
Title: expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25236
Title: expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25315
Title: expat: Integer overflow in storeRawNames()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22822
Title: expat: Integer overflow in addBinding in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22823
Title: expat: Integer overflow in build_model in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-22824
Title: expat: Integer overflow in defineAttribute in xmlparse.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23852
```

```
Title: expat: Integer overflow in function XML_GetBuffer
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25235
Title: expat: Malformed 2- and 3-byte UTF-8 sequences can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25236
Title: expat: Namespace-separator characters in "xmlns[:prefix]" attribute values can lead to arbitrary code execution
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-25315
Title: expat: Integer overflow in storeRawNames()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-17456
Title: git: arbitrary code execution via .gitmodules
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-19486
Title: git: Improper handling of PATH allows for commands to be executed from the current directory
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-16428
Title: glib2: NULL pointer dereference in g_markup_parse_context_end_parse() function in gmarkup.c
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-12450
Title: glib2: file_copy_fallback in gio/gfile.c in GNOME GLib does not properly restrict file permissions while a copy
operation is in progress
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9169
Title: glibc: regular-expression match via proceed_next_node in posix/regexec.c leads to heap-based buffer over-read
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-33574
Title: glibc: mq_notify does not handle separately allocated thread attributes
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-35942
Title: glibc: Arbitrary read in wordexp()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23218
Title: glibc: Stack-based buffer overflow in svcunix_create via long pathnames
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23219
Title: glibc: Stack-based buffer overflow in sunrpc clnt_create via a long pathname
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9169
Title: glibc: regular-expression match via proceed_next_node in posix/regexec.c leads to heap-based buffer over-read
```

```
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-33574
Title: glibc: mq_notify does not handle separately allocated thread attributes
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-35942
Title: glibc: Arbitrary read in wordexp()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23218
Title: glibc: Stack-based buffer overflow in svcunix_create via long pathnames
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23219
Title: glibc: Stack-based buffer overflow in sunrpc clnt_create via a long pathname
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-14809
Title: golang: malformed hosts in URLs leads to authorization bypass
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2021-38297
Title: golang: Command-line arguments may overwrite global data
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-23806
Title: golang: crypto/elliptic: IsOnCurve returns true for invalid field elements
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3858
Title: libssh2: Zero-byte allocation with a specially crafted SFTP packed leading to an out-of-bounds read
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3859
Title: libssh2: Unchecked use of _libssh2_packet_require and _libssh2_packet_requirev resulting in out-of-bounds read
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3860
Title: libssh2: Out-of-bounds reads with specially crafted SFTP packets
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3861
Title: libssh2: Out-of-bounds reads with specially crafted SSH packets
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-3862
Title: libssh2: Out-of-bounds memory comparison with specially crafted message channel request
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-12403
Title: nss: CHACHA20-POLY1305 decryption with undersized tag leads to out-of-bounds read
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
```

```
VulnerabilityID: CVE-2021-43527
Title: nss: Memory corruption in decodeECorDsaSignature with DSA signatures (and RSA-PSS)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-2938
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, and 8u181 (Java DB)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-3183
Title: OpenJDK: Unrestricted access to scripting engine (Scripting, 8202936)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-2938
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, and 8u181 (Java DB)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-3183
Title: OpenJDK: Unrestricted access to scripting engine (Scripting, 8202936)
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-29155
Title: openldap: OpenLDAP SQL injection
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-1292
Title: openssl: c_rehash script allows command injection
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-2068
Title: openssl: the c_rehash script allows command injection
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-1292
Title: openssl: c_rehash script allows command injection
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-2068
Title: openssl: the c_rehash script allows command injection
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-18311
Title: perl: Integer overflow leading to buffer overflow in Perl_my_setenv()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-18312
Title: perl: Heap-based buffer overflow in S_handle_regex_sets()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-18313
Title: perl: Heap-based buffer read overflow in S_grok_bslash_N()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-18314
Title: perl: Heap-based buffer overflow in S_regatom()
```

```
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1126
Title: procps-ng, procps: incorrect integer size in proc/alloc.* leading to truncation / integer overflow issues
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000802
Title: python: Command injection in the shutil module
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-10160
Title: python: regression of CVE-2019-9636 due to functional fix to allow port numbers in netloc
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9636
Title: python: Information Disclosure due to urlsplit improper NFKC normalization
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9948
Title: python: Undocumented local_file protocol allows remote attackers to bypass protection mechanisms
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000802
Title: python: Command injection in the shutil module
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-10160
Title: python: regression of CVE-2019-9636 due to functional fix to allow port numbers in netloc
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9636
Title: python: Information Disclosure due to urlsplit improper NFKC normalization
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9948
Title: python: Undocumented local_file protocol allows remote attackers to bypass protection mechanisms
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2018-1000802
Title: python: Command injection in the shutil module
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-10160
Title: python: regression of CVE-2019-9636 due to functional fix to allow port numbers in netloc
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9636
Title: python: Information Disclosure due to urlsplit improper NFKC normalization
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-9948
Title: python: Undocumented local_file protocol allows remote attackers to bypass protection mechanisms
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
```

```
VulnerabilityID: CVE-2019-19317
Title: sqlite: omits bits from the colUsed bitmask in the case of a generated column
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-19646
Title: sqlite: pragma.c mishandles NOT NULL in an integrity_check PRAGMA command in certain cases of generated columns
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-8457
Title: sqlite: heap out-of-bound read in function rtreenode()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-11656
Title: sqlite: use-after-free in the ALTER TABLE implementation
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-19317
Title: sqlite: omits bits from the colUsed bitmask in the case of a generated column
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-19646
Title: sqlite: pragma.c mishandles NOT NULL in an integrity_check PRAGMA command in certain cases of generated columns
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-8457
Title: sqlite: heap out-of-bound read in function rtreenode()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-11656
Title: sqlite: use-after-free in the ALTER TABLE implementation
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-19317
Title: sqlite: omits bits from the colUsed bitmask in the case of a generated column
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-19646
Title: sqlite: pragma.c mishandles NOT NULL in an integrity_check PRAGMA command in certain cases of generated columns
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2019-8457
Title: sqlite: heap out-of-bound read in function rtreenode()
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-11656
Title: sqlite: use-after-free in the ALTER TABLE implementation
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2022-37434
Title: zlib: heap-based buffer over-read and overflow in inflate() in inflate.c via a large gzip header extra field
Peso: 2 - Monitorare e pianificare l'intervento
```

```
-------------------
VulnerabilityID: CVE-2022-37434
Title: zlib: heap-based buffer over-read and overflow in inflate() in inflate.c via a large gzip header extra field
Peso: 2 - Monitorare e pianificare l'intervento
-------------------
VulnerabilityID: CVE-2020-11979
Title: ant: insecure temporary file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1945
Title: ant: insecure temporary file vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36373
Title: ant: excessive memory allocation when reading a specially crafted TAR archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36374
Title: ant: excessive memory allocation when reading a specially crafted ZIP archive or a derived formats
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8014
Title: tomcat: Insecure defaults in CORS filter enable 'supportsCredentials' for all origins
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1336
Title: tomcat: A bug in the UTF-8 decoder can lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8034
Title: tomcat: Host name verification missing in WebSocket client
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-0199
Title: tomcat: Apache Tomcat HTTP/2 DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-10072
Title: tomcat: HTTP/2 connection window exhaustion on write, incomplete fix of CVE-2019-0199
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-12418
Title: tomcat: local privilege escalation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17563
Title: tomcat: Session fixation when using FORM authentication
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-11996
Title: tomcat: specially crafted sequence of HTTP/2 requests can lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13934
```

```
Title: tomcat: OutOfMemoryException caused by HTTP/2 connection leak could lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13935
Title: tomcat: multiple requests with invalid payload length in a WebSocket frame could lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-17527
Title: tomcat: HTTP/2 request header mix-up
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-9484
Title: tomcat: deserialization flaw in session persistence storage leading to RCE
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-25122
Title: tomcat: Request mix-up with h2c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-25329
Title: tomcat: Incomplete fix for CVE-2020-9484 (RCE via session persistence)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-41079
Title: tomcat: Infinite loop while reading an unexpected TLS packet when using OpenSSL JSSE engine
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-42340
Title: tomcat: OutOfMemoryError caused by HTTP upgrade connection leak could lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23181
Title: tomcat: local privilege escalation vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8037
Title: tomcat: Due to a mishandling of close in NIO/NIO2 connectors user sessions can get mixed up
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17569
Title: tomcat: Regression in handling of Transfer-Encoding header allows for HTTP request smuggling
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13943
Title: tomcat: Apache Tomcat HTTP/2 Request mix-up
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1935
Title: tomcat: Mishandling of Transfer-Encoding header allows for HTTP request smuggling
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-30640
Title: tomcat: JNDI realm authentication weakness
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2021-33037
Title: tomcat: HTTP request smuggling when used with a reverse proxy
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18276
Title: bash: when effective UID is not equal to its real UID the saved UID is not dropped
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000876
Title: binutils: integer overflow leads to heap-based buffer overflow in objdump
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-19931
Title: binutils: Heap-based buffer overflow in bfd_elf32_swap_phdr_in function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-6543
Title: binutils:  integer overflow in load_specific_debug_section function in objdump.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7208
Title: binutils: Improper bounds check in coffgen.c:coff_pointerize_aux() allows for denial of service when parsing a
crafted COFF file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7643
Title: binutils: Integer overflow in the display_debug_ranges function resulting in crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9075
Title: binutils: heap-based buffer overflow in function _bfd_archive_64_bit_slurp_armap in archive64.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9077
Title: binutils: heap-based buffer overflow in function process_mips_specific in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-45078
Title: binutils: out-of-bounds write in stab_xcoff_builtin_type() in stabs.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-14930
Title: binutils: Memory leak in decode_line_info
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-14932
Title: binutils: Infinite loop in the decode_line_info
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-14933
Title: binutils: Infinite loop in read_formatted_entries
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

VulnerabilityID: CVE-2017-14934
Title: binutils: Infinite loop in process_debug_info
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-14938
Title: binutils: Excessive memory allocation in _bfd_elf_slurp_version_tables
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-14939
Title: binutils: Heap-based buffer over-read in the decode_line_info
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-14940
Title: binutils: NULL pointer dereference in the scan_unit_for_symbols
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-14974
Title: binutils: NULL pointer dereference in the *_get_synthetic_symtab functions
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-17080
Title: binutils: Heap-based buffer over-read in bfd_getl32
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2017-17123
Title: binutils: NULL pointer dereference in the coff_slurp_reloc_table function
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-10372
Title: binutils: Heap-base buffer over-read in dwarf.c:process_cu_tu_index() allows for denial of service via crafted file
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-10373
Title: binutils: NULL pointer dereference in dwarf2.c:concat_filename() allows for denial of service via crafted file
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-10534
Title: binutils: out of bounds memory write in peXXigen.c files
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-10535
Title: binutils: NULL pointer dereference in elf.c
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-17358
Title: binutils: invalid memory access in _bfd_stab_section_find_nearest_line in syms.c
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-17359
Title: binutils: invalid memory access in bfd_zalloc in opncls.c
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-17360
Title: binutils: heap-based buffer over-read in bfd_getl32 in libbfd.c

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-17794
Title: binutils: NULL pointer dereference in libiberty/cplus-dem.c:work_stuff_copy_to_from() via crafted input
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18309
Title: binutils: invalid memory address dereference in read_reloc in reloc.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18484
Title: binutils: Stack exhaustion in cp-demangle.c allows for denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18605
Title: binutils: heap-based buffer over-read in sec_merge_hash_lookup in merge.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18606
Title: binutils: NULL pointer dereference in _bfd_add_merge_section in merge_strings function in merge.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18607
Title: binutils: NULL pointer dereference in elf_link_input_bfd in elflink.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18700
Title: binutils: Recursive Stack Overflow within function d_name, d_encoding, and d_local_name in cp-demangle.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18701
Title: binutils: infinite recursion in next_is_type_qual and cplus_demangle_type functions in cp-demangle.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-19932
Title: binutils: Integer overflow due to the IS_CONTAINED_BY_LMA macro resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20002
Title: binutils: memory leak in _bfd_generic_read_minisymbols function in syms.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20623
Title: binutils: Use-after-free in the error function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20651
Title: binutils: NULL pointer dereference in elf_link_add_object_symbols function resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20671
Title: binutils: Integer overflow in load_specific_debug_section function
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2018-6759
Title: binutils: Unchecked strnlen in opncls.c:bfd_get_debug_link_info_1() can allow lead to denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-6872
Title: binutils: out of bounds read in elf_parse_notes function in elf.c file in libbfd library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7568
Title: binutils: integer overflow via an ELF file with corrupt dwarf1 debug information in libbfd library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7569
Title: binutils: integer underflow or overflow via an ELF file with a corrupt DWARF FORM block in libbfd library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7570
Title: binutils: NULL pointer dereference the assign_file_positions_for_non_load_sections function in libbfd library
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7642
Title: binutils: NULL pointer dereference in swap_std_reloc_in function in aoutx.h resulting in crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8945
Title: binutils: Crash in elf.c:bfd_section_from_shdr() with crafted executable
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-2019-12972
Title: binutils: out-of-bounds read in setup_group in bfd/elf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-14250
Title: binutils: integer overflow in simple-object-elf.c leads to a heap-based buffer overflow
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-14444
Title: binutils: integer overflow in function apply_relocation in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17450
Title: binutils: denial of service via crafted ELF file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17451
Title: binutils: integer overflow leading to a SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9071
```

```
Title: binutils: stack consumption in function d_count_templates_scopes in cp-demangle.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9073
Title: binutils: excessive memory allocation in function _bfd_elf_slurp_version_tables in elf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9074
Title: binutils: out-of-bound read in function bfd_getl32 in libbfd.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35493
Title: binutils: heap-based buffer overflow in bfd_pef_parse_function_stubs function in bfd/pef.c via crafted PEF file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35494
Title: binutils: usage of unitialized heap in tic4x_print_cond function in opcodes/tic4x-dis.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35495
Title: binutils: NULL pointer dereference in bfd_pef_parse_symbols function in bfd/pef.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35496
Title: binutils: NULL pointer dereference in bfd_pef_scan_start_address function in bfd/pef.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35507
Title: binutils: NULL pointer dereference in bfd_pef_parse_function_stubs function in bfd/pef.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-38533
Title: binutils: heap-based buffer overflow in bfd_getl32() when called by strip_main() in objcopy.c via a crafted file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000301
Title: curl: Out-of-bounds heap read when missing RTSP headers allows information leak or denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16839
Title: curl: Integer overflow leading to heap-based buffer overflow in Curl_sasl_create_plain_message()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16840
Title: curl: Use-after-free when closing "easy" handle in Curl_close()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16842
Title: curl: Heap-based buffer over-read in the curl tool warning formatting
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3822
Title: curl: NTLMv2 type-3 header stack buffer overflow
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2019-5481
Title: curl: double free due to subsequent call of realloc()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16890
Title: curl: NTLM type-2 heap out-of-bounds buffer read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3823
Title: curl: SMTP end-of-response out-of-bounds read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5436
Title: curl: TFTP receive heap buffer overflow in tftp_receive_packet() function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8177
Title: curl: Incorrect argument check can allow remote servers to overwrite local files
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8231
Title: curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8285
Title: curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8286
Title: curl: Inferior OCSP verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22901
Title: curl: Use-after-free in TLS session handling when using OpenSSL TLS backend
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22926
Title: curl: CURLOPT_SSLCERT mixup with Secure Transport
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22946
Title: curl: Requirement to use TLS not properly enforced for IMAP, POP3, and FTP protocols
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22576
Title: curl: OAUTH2 bearer bypass in connection re-use
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27775
Title: curl: bad local IPv6 connection reuse
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27780
```

```
Title: curl: percent-encoded path separator in URL host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27781
Title: curl: CERTINFO never-ending busy-loop
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27782
Title: curl: TLS and SSH connection too eager reuse
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3221
Title: rdiffweb CSRF vulnerability in profile's SSH keys can lead to unauthorized access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42915
Title: curl: HTTP proxy double-free
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42916
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43551
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22876
Title: curl: Leak of authentication credentials in URL via automatic Referer
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22897
Title: curl: Cipher settings shared for all connections when using schannel TLS backed
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22925
Title: curl: Incorrect fix for CVE-2021-22898 TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22947
Title: curl: Server responses received before STARTTLS processed after TLS handshake
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27774
Title: curl: credential leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27776
Title: curl: auth/cookie leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27779
Title: curl: cookie for trailing dot TLD
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2022-30115
Title: curl: HSTS bypass via trailing dot
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32205
Title: curl: Set-Cookie denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32206
Title: curl: HTTP compression denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32208
Title: curl: FTP-KRB bad message verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35260
Title: curl: .netrc parser out-of-bounds access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43552
Title: curl: Use-after-free triggered by an HTTP proxy deny response
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8284
Title: curl: FTP PASV command response can cause curl to connect to arbitrary host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22890
Title: curl: TLS 1.3 session ticket mix-up with HTTPS proxy host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22898
Title: curl: TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22924
Title: curl: Bad connection reuse due to flawed path name checks
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35252
Title: curl: Incorrect handling of control code characters in cookies
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000301
Title: curl: Out-of-bounds heap read when missing RTSP headers allows information leak or denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16890
Title: curl: NTLM type-2 heap out-of-bounds buffer read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3823
```

```
Title: curl: SMTP end-of-response out-of-bounds read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5436
Title: curl: TFTP receive heap buffer overflow in tftp_receive_packet() function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8177
Title: curl: Incorrect argument check can allow remote servers to overwrite local files
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8231
Title: curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8285
Title: curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8286
Title: curl: Inferior OCSP verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22901
Title: curl: Use-after-free in TLS session handling when using OpenSSL TLS backend
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22926
Title: curl: CURLOPT_SSLCERT mixup with Secure Transport
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22946
Title: curl: Requirement to use TLS not properly enforced for IMAP, POP3, and FTP protocols
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22576
Title: curl: OAUTH2 bearer bypass in connection re-use
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27775
Title: curl: bad local IPv6 connection reuse
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27780
Title: curl: percent-encoded path separator in URL host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27781
Title: curl: CERTINFO never-ending busy-loop
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27782
Title: curl: TLS and SSH connection too eager reuse
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2022-3221
Title: rdiffweb CSRF vulnerability in profile's SSH keys can lead to unauthorized access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42915
Title: curl: HTTP proxy double-free
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42916
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43551
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22876
Title: curl: Leak of authentication credentials in URL via automatic Referer
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22897
Title: curl: Cipher settings shared for all connections when using schannel TLS backed
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22925
Title: curl: Incorrect fix for CVE-2021-22898 TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22947
Title: curl: Server responses received before STARTTLS processed after TLS handshake
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27774
Title: curl: credential leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27776
Title: curl: auth/cookie leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27779
Title: curl: cookie for trailing dot TLD
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-30115
Title: curl: HSTS bypass via trailing dot
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32205
Title: curl: Set-Cookie denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32206
```

```
Title: curl: HTTP compression denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32208
Title: curl: FTP-KRB bad message verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35260
Title: curl: .netrc parser out-of-bounds access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43552
Title: curl: Use-after-free triggered by an HTTP proxy deny response
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8284
Title: curl: FTP PASV command response can cause curl to connect to arbitrary host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22890
Title: curl: TLS 1.3 session ticket mix-up with HTTPS proxy host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22898
Title: curl: TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22924
Title: curl: Bad connection reuse due to flawed path name checks
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35252
Title: curl: Incorrect handling of control code characters in cookies
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16890
Title: curl: NTLM type-2 heap out-of-bounds buffer read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3823
Title: curl: SMTP end-of-response out-of-bounds read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5436
Title: curl: TFTP receive heap buffer overflow in tftp_receive_packet() function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8177
Title: curl: Incorrect argument check can allow remote servers to overwrite local files
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8231
Title: curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2020-8285
Title: curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8286
Title: curl: Inferior OCSP verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22901
Title: curl: Use-after-free in TLS session handling when using OpenSSL TLS backend
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22926
Title: curl: CURLOPT_SSLCERT mixup with Secure Transport
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22946
Title: curl: Requirement to use TLS not properly enforced for IMAP, POP3, and FTP protocols
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22576
Title: curl: OAUTH2 bearer bypass in connection re-use
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27775
Title: curl: bad local IPv6 connection reuse
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27780
Title: curl: percent-encoded path separator in URL host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27781
Title: curl: CERTINFO never-ending busy-loop
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27782
Title: curl: TLS and SSH connection too eager reuse
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-3221
Title: rdiffweb CSRF vulnerability in profile's SSH keys can lead to unauthorized access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42915
Title: curl: HTTP proxy double-free
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-42916
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43551
```

```
Title: curl: HSTS bypass via IDN
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22876
Title: curl: Leak of authentication credentials in URL via automatic Referer
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22897
Title: curl: Cipher settings shared for all connections when using schannel TLS backed
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22925
Title: curl: Incorrect fix for CVE-2021-22898 TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22947
Title: curl: Server responses received before STARTTLS processed after TLS handshake
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27774
Title: curl: credential leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27776
Title: curl: auth/cookie leak on redirect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27779
Title: curl: cookie for trailing dot TLD
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-30115
Title: curl: HSTS bypass via trailing dot
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32205
Title: curl: Set-Cookie denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32206
Title: curl: HTTP compression denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32208
Title: curl: FTP-KRB bad message verification
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35260
Title: curl: .netrc parser out-of-bounds access
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43552
Title: curl: Use-after-free triggered by an HTTP proxy deny response
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2020-8284
Title: curl: FTP PASV command response can cause curl to connect to arbitrary host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22890
Title: curl: TLS 1.3 session ticket mix-up with HTTPS proxy host
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22898
Title: curl: TELNET stack contents disclosure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22924
Title: curl: Bad connection reuse due to flawed path name checks
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-35252
Title: curl: Incorrect handling of control code characters in cookies
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19906
Title: cyrus-sasl: denial of service in _sasl_add_string function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-24407
Title: cyrus-sasl: failure to properly escape SQL input allows an attacker to execute arbitrary SQL commands
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5094
Title: e2fsprogs: Crafted ext4 partition leads to out-of-bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5188
Title: e2fsprogs: Out-of-bounds write in e2fsck/rehash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5094
Title: e2fsprogs: Crafted ext4 partition leads to out-of-bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5188
Title: e2fsprogs: Out-of-bounds write in e2fsck/rehash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5094
Title: e2fsprogs: Crafted ext4 partition leads to out-of-bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5188
Title: e2fsprogs: Out-of-bounds write in e2fsck/rehash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16062
```

```
Title: elfutils: Heap-based buffer over-read in libdw/dwarf_getaranges.c:dwarf_getaranges() via crafted file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18310
Title: elfutils: invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18520
Title: elfutils: eu-size cannot handle recursive ar files
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18521
Title: elfutils: Divide-by-zero in arlib_add_symbols function in arlib.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7148
Title: elfutils: excessive memory allocation in read_long_names in elf_begin.c in libelf
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7149
Title: elfutils: heap-based buffer over-read in read_srclines in dwarf_getsrclines.c in libdw
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7150
Title: elfutils: segmentation fault in elf64_xlatetom in libelf/elf32_xlatetom.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16062
Title: elfutils: Heap-based buffer over-read in libdw/dwarf_getaranges.c:dwarf_getaranges() via crafted file
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18310
Title: elfutils: invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18520
Title: elfutils: eu-size cannot handle recursive ar files
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-18521
Title: elfutils: Divide-by-zero in arlib_add_symbols function in arlib.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7148
Title: elfutils: excessive memory allocation in read_long_names in elf_begin.c in libelf
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7149
Title: elfutils: heap-based buffer over-read in read_srclines in dwarf_getsrclines.c in libdw
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7150
Title: elfutils: segmentation fault in elf64_xlatetom in libelf/elf32_xlatetom.c
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2018-20843
Title: expat: large number of colons in input makes parser consume high amount of resources, leading to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-15903
Title: expat: heap-based buffer over-read via crafted XML input
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-45960
Title: expat: Large number of prefixed XML attributes on a single tag can crash libexpat
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-46143
Title: expat: Integer overflow in doProlog in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22825
Title: expat: Integer overflow in lookup in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22826
Title: expat: Integer overflow in nextScaffoldPart in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22827
Title: expat: Integer overflow in storeAtts in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23990
Title: expat: integer overflow in the doProlog function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25314
Title: expat: Integer overflow in copyString()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-40674
Title: expat: a use-after-free in the doContent function in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43680
Title: expat: use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25313
Title: expat: Stack exhaustion in doctype parsing
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20843
Title: expat: large number of colons in input makes parser consume high amount of resources, leading to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-15903
```

```
Title: expat: heap-based buffer over-read via crafted XML input
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-45960
Title: expat: Large number of prefixed XML attributes on a single tag can crash libexpat
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-46143
Title: expat: Integer overflow in doProlog in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22825
Title: expat: Integer overflow in lookup in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22826
Title: expat: Integer overflow in nextScaffoldPart in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22827
Title: expat: Integer overflow in storeAtts in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23990
Title: expat: integer overflow in the doProlog function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25314
Title: expat: Integer overflow in copyString()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-40674
Title: expat: a use-after-free in the doContent function in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43680
Title: expat: use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25313
Title: expat: Stack exhaustion in doctype parsing
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20843
Title: expat: large number of colons in input makes parser consume high amount of resources, leading to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-15903
Title: expat: heap-based buffer over-read via crafted XML input
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-45960
Title: expat: Large number of prefixed XML attributes on a single tag can crash libexpat
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2021-46143
Title: expat: Integer overflow in doProlog in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22825
Title: expat: Integer overflow in lookup in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22826
Title: expat: Integer overflow in nextScaffoldPart in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-22827
Title: expat: Integer overflow in storeAtts in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23990
Title: expat: integer overflow in the doProlog function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25314
Title: expat: Integer overflow in copyString()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-40674
Title: expat: a use-after-free in the doContent function in xmlparse.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-43680
Title: expat: use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-25313
Title: expat: Stack exhaustion in doctype parsing
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18218
Title: file: heap-based buffer overflow in cdf_read_property_info in cdf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8904
Title: file: stack-based buffer over-read in do_bid_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8907
Title: file: do_core_note in readelf.c allows remote attackers to cause a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8905
Title: file: stack-based buffer over-read in do_core_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8906
```

```
Title: file: out-of-bounds read in do_core_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18218
Title: file: heap-based buffer overflow in cdf_read_property_info in cdf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8904
Title: file: stack-based buffer over-read in do_bid_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8907
Title: file: do_core_note in readelf.c allows remote attackers to cause a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8905
Title: file: stack-based buffer over-read in do_core_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-8906
Title: file: out-of-bounds read in do_core_note in readelf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-11233
Title: git: path sanity check in is_ntfs_dotgit() can read arbitrary memory
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-11235
Title: git: arbitrary code execution when recursively cloning a malicious repository
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19604
Title: git: Recursive clone followed by a submodule update could execute code contained within repository without the
user explicitly consent
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-11008
Title: git: Crafted URL containing new lines, empty host or lacks a scheme can cause credential leak
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-5260
Title: git: Crafted URL containing new lines can cause credential leak
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-21300
Title: git: remote code execution during clone operation on case-insensitive filesystems
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-40330
Title: git: unexpected cross-protocol requests via a repository path containing a newline character
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-24765
Title: git: On multi-user machines Git users might find themselves unexpectedly in a Git worktree
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-24975
Title: git: The --mirror option for git leaks secret for deleted content, aka the "GitBleed"
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-39260
Title: git: git shell function that splits command arguments can lead to arbitrary heap writes.
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-39253
Title: git: exposure of sensitive information to a malicious actor
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16429
Title: glib2: Out-of-bounds read in g_markup_parse_context_parse() in gmarkup.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-13012
Title: glib2: insecure permissions for files and directories
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35457
Title: GNOME GLib before 2.65.3 has an integer overflow, that might lead to a ...
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-27218
Title: glib: integer overflow in g_byte_array_new_take function when called with a buffer of 4GB or more on a 64-bit platform
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-27219
Title: glib: integer overflow in g_bytes_new function on 64-bit platforms due to an implicit cast from 64 bits to 32 bits
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-28153
Title: glib: g_file_replace() with G_FILE_CREATE_REPLACE_DESTINATION creates empty target for dangling symlink
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3800
Title: glib2: Possible privilege escalation thourgh pkexec and aliases
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2009-5155
Title: glibc: parse_reg_exp in posix/regcomp.c misparses alternatives leading to denial of service or trigger incorrect result
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-19591
Title: glibc: file descriptor leak in if_nametoindex() in sysdeps/unix/sysv/linux/if_index.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1752
Title: glibc: use-after-free in glob() function when expanding ~user
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3326
Title: glibc: Assertion failure in ISO-2022-JP-3 gconv module related to combining characters
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-38604
Title: glibc: NULL pointer dereference in helper_thread() in mq_notify.c while handling NOTIFY_REMOVED messages
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3999
Title: glibc: Off-by-one buffer overflow/underflow in getcwd()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-25013
Title: glibc: buffer over-read in iconv when processing invalid multi-byte input sequences in the EUC-KR encoding
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7309
Title: glibc: memcmp function incorrectly returns zero
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-10029
Title: glibc: stack corruption from crafted input in cosl, sinl, sincosl, and tanl functions
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-27618
Title: glibc: iconv when processing invalid multi-byte input sequences fails to advance the input state, which could result in an infinite loop
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2009-5155
Title: glibc: parse_reg_exp in posix/regcomp.c misparses alternatives leading to denial of service or trigger incorrect result
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-19591
Title: glibc: file descriptor leak in if_nametoindex() in sysdeps/unix/sysv/linux/if_index.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1752
Title: glibc: use-after-free in glob() function when expanding ~user
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3326
Title: glibc: Assertion failure in ISO-2022-JP-3 gconv module related to combining characters
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-38604
Title: glibc: NULL pointer dereference in helper_thread() in mq_notify.c while handling NOTIFY_REMOVED messages
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3999
Title: glibc: Off-by-one buffer overflow/underflow in getcwd()
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-25013
Title: glibc: buffer over-read in iconv when processing invalid multi-byte input sequences in the EUC-KR encoding
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-7309
Title: glibc: memcmp function incorrectly returns zero
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-10029
Title: glibc: stack corruption from crafted input in cosl, sinl, sincosl, and tanl functions
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-27618
Title: glibc: iconv when processing invalid multi-byte input sequences fails to advance the input state, which could result in an infinite loop
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16873
Title: golang: "go get" command vulnerable to RCE via import of malicious package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16874
Title: golang: "go get" vulnerable to directory traversal via malicious package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16875
Title: golang: crypto/x509 allows for denial of service via crafted TLS client certificate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-17143
Title: golang-org-x-net-html: Runtime panic in html.Parse() via crafted html
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-17846
Title: golang-org-x-net-html: infinite loop during html.Parse() via inSelectIM and inSelectInTableIM
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-6574
Title: golang: arbitrary code execution during "go get" via C compiler options
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7187
Title: golang: arbitrary command execution via VCS path
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16276
Title: golang: HTTP/1.1 headers with a space before the colon leads to filter bypass or request smuggling
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17596
Title: golang: invalid public key causes panic in dsa.Verify
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2019-6486
Title: golang: crypto/elliptic implementations of P-521 and P-384 elliptic curves allow for denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-16845
Title: golang: ReadUvarint and ReadVarint can read an unlimited number of bytes from invalid inputs
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-28362
Title: golang: math/big: panic during recursive division of very large numbers
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-28366
Title: golang: malicious symbol names can lead to code execution at build time
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-28367
Title: golang: improper validation of cgo flags can lead to code execution at build time
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-7919
Title: golang: Integer overflow on 32bit architectures via crafted certificate allows for denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-27918
Title: golang: encoding/xml: infinite loop when using xml.NewTokenDecoder with a custom TokenReader
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-29923
Title: golang: net: incorrect parsing of extraneous zero characters at the beginning of an IP address octet
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-33194
Title: golang: x/net/html: infinite loop in ParseFragment
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-33195
Title: golang: net: lookup functions may return invalid host names
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-33196
Title: golang: archive/zip: malformed archive may cause panic or memory exhaustion
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-33198
Title: golang: math/big.Rat: may cause a panic or an unrecoverable fatal error if passed inputs with very large exponents
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-41771
Title: golang: debug/macho: invalid dynamic symbol table command can cause panic
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-41772
```

```
Title: golang: archive/zip: Reader.Open panics on empty string
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-44716
Title: golang: net/http: limit growth of header canonicalization cache
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23772
Title: golang: math/big: uncontrolled memory consumption due to an unhandled overflow via Rat.SetString
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23773
Title: golang: cmd/go: misinterpretation of branch names can lead to incorrect access control
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-24675
Title: golang: encoding/pem: fix stack overflow in Decode
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-24921
Title: golang: regexp: stack exhaustion via a deeply nested expression
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-27664
Title: golang: net/http: handle server errors after sending GOAWAY
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-28131
Title: golang: encoding/xml: stack exhaustion in Decoder.Skip
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-28327
Title: golang: crypto/elliptic: panic caused by oversized scalar
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-2879
Title: golang: archive/tar: unbounded memory consumption when reading headers
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-2880
Title: golang: net/http/httputil: ReverseProxy should not forward unparseable query parameters
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-29804
Title: ELSA-2022-17957: ol8addon security update (IMPORTANT)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-30580
Title: golang: os/exec: Code injection in Cmd.Start
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-30630
Title: golang: io/fs: stack exhaustion in Glob
Peso: 1 - Monitorare la vulnerabilità
```

VulnerabilityID: CVE-2022-30631
Title: golang: compress/gzip: stack exhaustion in Reader.Read
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-30632
Title: golang: path/filepath: stack exhaustion in Glob
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-30633
Title: golang: encoding/xml: stack exhaustion in Unmarshal
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-30635
Title: golang: encoding/gob: stack exhaustion in Decoder.Decode
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-32189
Title: golang: math/big: decoding big.Float and big.Rat types can panic if the encoded message is too short, potentially allowing a denial of service
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-41715
Title: golang: regexp/syntax: limit memory used by parsing regexps
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2022-41716
Title: Due to unsanitized NUL values, attackers may be able to maliciously se ...
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-9741
Title: golang: CRLF injection in net/http
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-15586
Title: golang: data race in certain net/http servers including ReverseProxy can lead to DoS
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-24553
Title: golang: default Content-Type setting in net/http/cgi and net/http/fcgi could cause XSS
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-29510
Title: go: encoding/xml: XML directives instability
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2021-3114
Title: golang: crypto/elliptic: incorrect operations on the P-224 curve
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2021-31525
Title: golang: net/http: panic in ReadRequest and ReadResponse when reading a very large header
Peso: 1 - Monitorare la vulnerabilità

```
VulnerabilityID: CVE-2021-33197
Title: golang: net/http/httputil: ReverseProxy forwards connection headers if first one is empty
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-34558
Title: golang: crypto/tls: certificate of wrong type is causing TLS client to panic
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36221
Title: golang: net/http/httputil: panic due to racy read of persistConn after handler panic
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-44717
Title: golang: syscall: don't close fd 0 on ForkExec error
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-1705
Title: golang: net/http: improper sanitization of Transfer-Encoding header
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-1962
Title: golang: go/parser: stack exhaustion in all Parse* functions
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-29526
Title: golang: syscall: faccessat checks wrong group
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-32148
Title: golang: net/http/httputil: NewSingleHostReverseProxy - omit X-Forwarded-For not working
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-30629
Title: golang: crypto/tls: session tickets lack random ticket_age_add
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-28196
Title: krb5: unbounded recursion via an ASN.1-encoded Kerberos message in lib/krb5/asn.1/asn1_encode.c may lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36222
Title: krb5: Sending a request containing PA-ENCRYPTED-CHALLENGE padata element without using FAST could result in NULL dereference in KDC which leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20217
Title: krb5: Reachable assertion in the KDC using S4U2Self requests
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-5729
Title: krb5: null dereference in kadmind or DN container check bypass by supplying special crafted data
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2021-37750
Title: krb5: NULL pointer dereference in process_tgs_req() in kdc/do_tgs_req.c via a FAST inner body that lacks server field
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-28196
Title: krb5: unbounded recursion via an ASN.1-encoded Kerberos message in lib/krb5/asn.1/asn1_encode.c may lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36222
Title: krb5: Sending a request containing PA-ENCRYPTED-CHALLENGE padata element without using FAST could result in NULL dereference in KDC which leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20217
Title: krb5: Reachable assertion in the KDC using S4U2Self requests
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-5729
Title: krb5: null dereference in kadmind or DN container check bypass by supplying special crafted data
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-37750
Title: krb5: NULL pointer dereference in process_tgs_req() in kdc/do_tgs_req.c via a FAST inner body that lacks server field
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000877
Title: libarchive: Double free in RAR decoder resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000878
Title: libarchive: Use after free in RAR decoder resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18408
Title: libarchive: use-after-free in archive_read_format_rar_read_data when there is an error in the decompression of an archive entry
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23177
Title: libarchive: extracting a symlink with ACLs modifies ACLs of target
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-31566
Title: libarchive: symbolic links incorrectly followed when changing modes, times, ACL and flags of a file while extracting an archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1000879
Title: libarchive: NULL pointer dereference in ACL parser resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2018-1000880
Title: libarchive: Improper input validation in WARC parser resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1000019
Title: libarchive: Out of bounds read in archive_read_support_format_7zip.c resulting in a denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1000020
Title: libarchive: Infinite recursion in archive_read_support_format_iso9660.c resulting in denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19221
Title: libarchive: out-of-bounds read in archive_wstring_append_from_mbs in archive_string.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-21674
Title: libarchive: heap-based buffer overflow in archive_string_append_from_wcs function in archive_string.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36084
Title: libsepol: use-after-free in __cil_verify_classperms()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36085
Title: libsepol: use-after-free in __cil_verify_classperms()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-36086
Title: libsepol: use-after-free in cil_reset_classpermission()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20387
Title: libsolv: out-of-bounds read in repodata_schema2id in repodata.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20532
Title: libsolv: NULL pointer dereference in function testcase_read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20533
Title: libsolv: NULL pointer dereference in function testcase_str2dep_complex
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20534
Title: libsolv: illegal address access in pool_whatprovides in src/pool.h
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3200
Title: libsolv: heap-based buffer overflow in testcase_read() in src/testcase.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-13115
Title: libssh2: integer overflow in kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c leads to
```

```
out-of-bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17498
Title: libssh2: integer overflow in SSH_MSG_DISCONNECT logic in packet.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3855
Title: libssh2: Integer overflow in transport read resulting in out of bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3856
Title: libssh2: Integer overflow in keyboard interactive handling resulting in out of bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3857
Title: libssh2: Integer overflow in SSH packet processing channel resulting in out of bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-3863
Title: libssh2: Integer overflow in user authenticate keyboard interactive allows out-of-bounds writes
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-14404
Title: libxml2: NULL pointer dereference in xmlXPathCompOpEval() function in xpath.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19956
Title: libxml2: memory leak in xmlParseBalancedChunkMemoryRecover in parser.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20388
Title: libxml2: memory leak in xmlSchemaPreRun in xmlschemas.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-7595
Title: libxml2: infinite loop in xmlStringLenDecodeEntities in some end-of-file situations
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3517
Title: libxml2: Heap-based buffer overflow in xmlEncodeEntitiesInternal() in entities.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3518
Title: libxml2: Use-after-free in xmlXIncludeDoProcess() in xinclude.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-2309
Title: lxml: NULL Pointer Dereference in lxml
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-23308
Title: libxml2: Use-after-free of ID and IDREF attributes
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2022-40303
Title: libxml2: integer overflows with XML_PARSE_HUGE
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-40304
Title: libxml2: dict corruption caused by entity reference cycles
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-24977
Title: libxml2: Buffer overflow vulnerability in xmlEncodeEntitiesInternal() in entities.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3537
Title: libxml2: NULL pointer dereference when post-validating mixed content parsed in recovery mode
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-29824
Title: libxml2: integer overflows in xmlBuf and xmlBuffer lead to out-of-bounds write
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-10754
Title: ncurses: NULL Pointer Dereference in _nc_parse_entry function in tinfo/parse_entry.c.
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-39537
Title: ncurses: heap-based buffer overflow in _nc_captoinfo() in captoinfo.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-29458
Title: ncurses: segfaulting OOB read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17594
Title: ncurses: heap-based buffer overflow in the _nc_find_entry function in tinfo/comp_hash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17595
Title: ncurses: heap-based buffer overflow in the fmt_entry function in tinfo/comp_hash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-10754
Title: ncurses: NULL Pointer Dereference in _nc_parse_entry function in tinfo/parse_entry.c.
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-39537
Title: ncurses: heap-based buffer overflow in _nc_captoinfo() in captoinfo.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-29458
Title: ncurses: segfaulting OOB read
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17594
```

```
Title: ncurses: heap-based buffer overflow in the _nc_find_entry function in tinfo/comp_hash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17595
Title: ncurses: heap-based buffer overflow in the fmt_entry function in tinfo/comp_hash.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12116
Title: nodejs: HTTP request splitting
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12121
Title: nodejs: Denial of Service with large HTTP headers
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12122
Title: nodejs: Slowloris HTTP Denial of Service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7161
Title: nodejs: denial of service (DoS) by causing a node server providing an http2 server to crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7167
Title: nodejs: Denial of Service by calling Buffer.fill() or Buffer.alloc() with specially crafted parameters
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5737
Title: nodejs: Insufficient Slowloris fix causing DoS via server.headersTimeout bypass
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8174
Title: nodejs: memory corruption in napi_get_value_string_* functions
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8252
Title: libuv: buffer overflow in realpath
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8265
Title: nodejs: use-after-free in the TLS implementation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22883
Title: nodejs: HTTP2 'unknownProtocol' cause DoS by resource exhaustion
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-22884
Title: nodejs: DNS rebinding in --inspect
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-44531
Title: nodejs: Improper handling of URI Subject Alternative Names
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2022-0778
Title: openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-21824
Title: nodejs: Prototype pollution via console.table properties
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-0734
Title: openssl: timing side channel attack in the DSA signature algorithm
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12123
Title: nodejs: Hostname spoofing in URL parser for javascript protocol
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8287
Title: nodejs: HTTP request smuggling via two copies of a header field in an http request
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-44532
Title: nodejs: Certificate Verification Bypass via String Injection
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-44533
Title: nodejs: Incorrect handling of certificate subject and issuer fields
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12384
Title: nss: ServerHello.random is all zeros when handling a v2-compatible ClientHello
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-12404
Title: nss: Cache side-channel variant of the Bleichenbacher attack
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2627
Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Installer)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2633
Title: OpenJDK: LDAPCertStore insecure handling of LDAP referrals (JNDI, 8186606)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2637
Title: OpenJDK: SingleEntryRegistry incorrect setup of deserialization filter (JMX, 8186998)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2638
Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2639
```

Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Deployment)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2794
Title: OpenJDK: unrestricted deserialization of data from JCEKS key stores (Security, 8189997)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2811
Title: Oracle JDK: unspecified vulnerability fixed in 8u171 and 10.0.1 (Install)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2814
Title: OpenJDK: incorrect handling of Reference clones can lead to sandbox bypass (Hotspot, 8192025)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2825
Title: OpenJDK: insufficient array type checks in VarHandle (Libraries, 8194233)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2826
Title: OpenJDK: incorrect type check for the MethodHandles' tryFinally cleanup exception type (Libraries, 8194238)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2941
Title: Oracle JDK: unspecified vulnerability fixed in 7u191, 8u181, and 10.0.2 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2942
Title: Oracle JDK: unspecified vulnerability fixed in 7u191 and 8u181 (Windows DLL)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-2964
Title: Oracle JDK: unspecified vulnerability fixed in 8u181 and 10.0.2 (Deployment)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-3149
Title: OpenJDK: Incomplete enforcement of the trustURLCodebase restriction (JNDI, 8199177)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-3169
Title: OpenJDK: Improper field access checks (Hotspot, 8199226)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-3209
Title: Oracle JDK: unspecified vulnerability fixed in 8u191 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2602
Title: OpenJDK: Slow conversion of BigDecimal to long (Libraries, 8211936)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2697
Title: Oracle JDK: Unspecified vulnerability fixed in 7u221 and 8u211 (2D)
Peso: 1 - Monitorare la vulnerabilità

```
-------------------
VulnerabilityID: CVE-2019-2698
Title: OpenJDK: Font layout engine out of bounds access setCurrGlyphID() (2D, 8219022)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14583
Title: OpenJDK: Bypass of boundary checks in nio.Buffer via concurrent access (Libraries, 8238920)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14593
Title: OpenJDK: Incomplete bounds checks in Affine Transformations (2D, 8240119)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2803
Title: OpenJDK: Incorrect bounds checks in NIO Buffers (Libraries, 8234841)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2805
Title: OpenJDK: Incorrect type checks in MethodType.readObject() (Libraries, 8235274)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2816
Title: OpenJDK: Application data accepted before TLS handshake completion (JSSE, 8235691)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2581
Title: Oracle JDK: unspecified vulnerability fixed in 7u171, 8u161, and 9.0.4 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2582
Title: OpenJDK: insufficient validation of the invokeinterface instruction (Hotspot, 8174962)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2588
Title: OpenJDK: LdapLoginModule insufficient username encoding in LDAP query (LDAP, 8178449)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2599
Title: OpenJDK: DnsClient missing source port randomization (JNDI, 8182125)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2602
Title: OpenJDK: loading of classes from untrusted locations (I18n, 8182601)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2603
Title: OpenJDK: DerValue unbounded memory allocation (Libraries, 8182387)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2618
Title: OpenJDK: insufficient strength of key agreement (JCE, 8185292)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2629
```

```
Title: OpenJDK: GSS context use-after-free (JGSS, 8186212)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2634
Title: OpenJDK: use of global credentials for HTTP/SPNEGO (JGSS, 8186600)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2641
Title: OpenJDK: GTK library loading use-after-free (AWT, 8185325)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2663
Title: OpenJDK: ArrayBlockingQueue deserialization to an inconsistent state (Libraries, 8189284)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2677
Title: OpenJDK: unbounded memory allocation during deserialization (AWT, 8190289)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2678
Title: OpenJDK: unbounded memory allocation in BasicAttributes deserialization (JNDI, 8191142)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2795
Title: OpenJDK: insufficient consistency checks in deserialization of multiple classes (Security, 8189977)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2796
Title: OpenJDK: unbounded memory allocation during deserialization in PriorityBlockingQueue (Concurrency, 8189981)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2797
Title: OpenJDK: unbounded memory allocation during deserialization in TabularDataSupport (JMX, 8189985)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2798
Title: OpenJDK: unbounded memory allocation during deserialization in Container (AWT, 8189989)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2799
Title: OpenJDK: unbounded memory allocation during deserialization in NamedNodeMapImpl (JAXP, 8189993)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2815
Title: OpenJDK: unbounded memory allocation during deserialization in StubIORImpl (Serialization, 8192757)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2940
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, 8u181, and 10.0.2 (Libraries)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2972
Title: OpenJDK: GCTR counter roll over (Security, 8200332)
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2018-2973
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, 8u181, and 10.0.2 (JSSE)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3180
Title: OpenJDK: Missing endpoint identification algorithm check during TLS session resumption (JSSE, 8202613)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3211
Title: Oracle JDK: unspecified vulnerability fixed in 8u191 and 11.0.1 (Serviceability)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3214
Title: OpenJDK: Infinite loop in RIFF format reader (Sound, 8205361)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2684
Title: OpenJDK: Incorrect skeleton selection in RMI registry server-side dispatch handling (RMI, 8218453)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2745
Title: OpenJDK: Side-channel attack risks in Elliptic Curve (EC) cryptography (Security, 8208698)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2762
Title: OpenJDK: Insufficient checks of suppressed exceptions in deserialization (Utilities, 8212328)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2769
Title: OpenJDK: Unbounded memory allocation during deserialization in Collections (Utilities, 8213432)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2816
Title: OpenJDK: Missing URL format validation (Networking, 8221518)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2821
Title: OpenJDK: Incorrect handling of certificate status messages during TLS handshake (JSSE, 8222678)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14556
Title: OpenJDK: Incorrect handling of access control context in ForkJoinPool (Libraries, 8237117)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14562
Title: OpenJDK: Excessive memory usage in ImageIO TIFF plugin (ImageIO, 8233239)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14621
Title: OpenJDK: XML validation manipulation due to incomplete application of the use-grammar-pool-only feature (JAXP,
8242136)
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2020-2767
Title: OpenJDK: Incorrect handling of Certificate messages during TLS handshake (JSSE, 8232581)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2781
Title: OpenJDK: Re-use of single TLS session for new connections (JSSE, 8234408)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2800
Title: OpenJDK: CRLF injection into HTTP headers in HttpServer (Lightweight HTTP Server, 8234825)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2830
Title: OpenJDK: Regular expression DoS in Scanner (Concurrency, 8236201)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2422
Title: OpenJDK: memory disclosure in FileChannelImpl (Libraries, 8206290)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2426
Title: OpenJDK: transparent NTLM authentication enabled by default (Networking, 8209094)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2449
Title: Oracle JDK: unspecified vulnerability fixed in 8u201 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2766
Title: OpenJDK: Insufficient permission checks for file:// URLs on Windows (Networking, 8213431)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2786
Title: OpenJDK: Insufficient restriction of privileges in AccessController (Security, 8216381)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2818
Title: OpenJDK: Non-constant time comparison in ChaCha20Cipher (Security, 8221344)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2842
Title: OpenJDK: Missing array bounds check in crypto providers (JCE, 8223511)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14573
Title: OpenJDK: Incomplete interface type checks in Graal compiler (Hotspot, 8236867)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14577
Title: OpenJDK: HostnameChecker does not ensure X.509 certificate names are in normalized form (JSSE, 8237592)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14581
Title: OpenJDK: Information disclosure in color management (2D, 8238002)
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2754
Title: OpenJDK: Misplaced regular expression syntax error check in RegExpScanner (Scripting, 8223898)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2755
Title: OpenJDK: Incorrect handling of empty string nodes in regular expression Parser (Scripting, 8223904)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2756
Title: OpenJDK: Incorrect handling of references to uninitialized class descriptors during deserialization (Serialization,
8224541)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2757
Title: OpenJDK: Uncaught InstantiationError exception in ObjectStreamClass (Serialization, 8224549)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2773
Title: OpenJDK: Unexpected exceptions raised by DOMKeyInfoFactory and DOMXMLSignatureFactory (Security,
8231415)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2778
Title: OpenJDK: Incomplete enforcement of algorithm restrictions for TLS (JSSE, 8232424)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2627
Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Installer)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2633
Title: OpenJDK: LDAPCertStore insecure handling of LDAP referrals (JNDI, 8186606)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2637
Title: OpenJDK: SingleEntryRegistry incorrect setup of deserialization filter (JMX, 8186998)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2638
Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2639
Title: Oracle JDK: unspecified vulnerability fixed in 8u161 and 9.0.4 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2794
Title: OpenJDK: unrestricted deserialization of data from JCEKS key stores (Security, 8189997)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2811
Title: Oracle JDK: unspecified vulnerability fixed in 8u171 and 10.0.1 (Install)
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2814
Title: OpenJDK: incorrect handling of Reference clones can lead to sandbox bypass (Hotspot, 8192025)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2825
Title: OpenJDK: insufficient array type checks in VarHandle (Libraries, 8194233)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2826
Title: OpenJDK: incorrect type check for the MethodHandles' tryFinally cleanup exception type (Libraries, 8194238)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2941
Title: Oracle JDK: unspecified vulnerability fixed in 7u191, 8u181, and 10.0.2 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2942
Title: Oracle JDK: unspecified vulnerability fixed in 7u191 and 8u181 (Windows DLL)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2964
Title: Oracle JDK: unspecified vulnerability fixed in 8u181 and 10.0.2 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3149
Title: OpenJDK: Incomplete enforcement of the trustURLCodebase restriction (JNDI, 8199177)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3169
Title: OpenJDK: Improper field access checks (Hotspot, 8199226)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3209
Title: Oracle JDK: unspecified vulnerability fixed in 8u191 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2602
Title: OpenJDK: Slow conversion of BigDecimal to long (Libraries, 8211936)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2697
Title: Oracle JDK: Unspecified vulnerability fixed in 7u221 and 8u211 (2D)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2698
Title: OpenJDK: Font layout engine out of bounds access setCurrGlyphID() (2D, 8219022)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14583
Title: OpenJDK: Bypass of boundary checks in nio.Buffer via concurrent access (Libraries, 8238920)
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2020-14593
Title: OpenJDK: Incomplete bounds checks in Affine Transformations (2D, 8240119)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2803
Title: OpenJDK: Incorrect bounds checks in NIO Buffers (Libraries, 8234841)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2805
Title: OpenJDK: Incorrect type checks in MethodType.readObject() (Libraries, 8235274)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2816
Title: OpenJDK: Application data accepted before TLS handshake completion (JSSE, 8235691)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2581
Title: Oracle JDK: unspecified vulnerability fixed in 7u171, 8u161, and 9.0.4 (JavaFX)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2582
Title: OpenJDK: insufficient validation of the invokeinterface instruction (Hotspot, 8174962)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2588
Title: OpenJDK: LdapLoginModule insufficient username encoding in LDAP query (LDAP, 8178449)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2599
Title: OpenJDK: DnsClient missing source port randomization (JNDI, 8182125)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2602
Title: OpenJDK: loading of classes from untrusted locations (I18n, 8182601)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2603
Title: OpenJDK: DerValue unbounded memory allocation (Libraries, 8182387)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2618
Title: OpenJDK: insufficient strength of key agreement (JCE, 8185292)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2629
Title: OpenJDK: GSS context use-after-free (JGSS, 8186212)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2634
Title: OpenJDK: use of global credentials for HTTP/SPNEGO (JGSS, 8186600)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2641
Title: OpenJDK: GTK library loading use-after-free (AWT, 8185325)
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2663
Title: OpenJDK: ArrayBlockingQueue deserialization to an inconsistent state (Libraries, 8189284)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2677
Title: OpenJDK: unbounded memory allocation during deserialization (AWT, 8190289)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2678
Title: OpenJDK: unbounded memory allocation in BasicAttributes deserialization (JNDI, 8191142)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2795
Title: OpenJDK: insufficient consistency checks in deserialization of multiple classes (Security, 8189977)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2796
Title: OpenJDK: unbounded memory allocation during deserialization in PriorityBlockingQueue (Concurrency, 8189981)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2797
Title: OpenJDK: unbounded memory allocation during deserialization in TabularDataSupport (JMX, 8189985)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2798
Title: OpenJDK: unbounded memory allocation during deserialization in Container (AWT, 8189989)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2799
Title: OpenJDK: unbounded memory allocation during deserialization in NamedNodeMapImpl (JAXP, 8189993)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2815
Title: OpenJDK: unbounded memory allocation during deserialization in StubIORImpl (Serialization, 8192757)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2940
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, 8u181, and 10.0.2 (Libraries)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2972
Title: OpenJDK: GCTR counter roll over (Security, 8200332)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-2973
Title: Oracle JDK: unspecified vulnerability fixed in 6u201, 7u191, 8u181, and 10.0.2 (JSSE)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-3180
Title: OpenJDK: Missing endpoint identification algorithm check during TLS session resumption (JSSE, 8202613)
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

VulnerabilityID: CVE-2018-3211
Title: Oracle JDK: unspecified vulnerability fixed in 8u191 and 11.0.1 (Serviceability)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-3214
Title: OpenJDK: Infinite loop in RIFF format reader (Sound, 8205361)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2684
Title: OpenJDK: Incorrect skeleton selection in RMI registry server-side dispatch handling (RMI, 8218453)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2745
Title: OpenJDK: Side-channel attack risks in Elliptic Curve (EC) cryptography (Security, 8208698)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2762
Title: OpenJDK: Insufficient checks of suppressed exceptions in deserialization (Utilities, 8212328)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2769
Title: OpenJDK: Unbounded memory allocation during deserialization in Collections (Utilities, 8213432)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2816
Title: OpenJDK: Missing URL format validation (Networking, 8221518)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-2821
Title: OpenJDK: Incorrect handling of certificate status messages during TLS handshake (JSSE, 8222678)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-14556
Title: OpenJDK: Incorrect handling of access control context in ForkJoinPool (Libraries, 8237117)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-14562
Title: OpenJDK: Excessive memory usage in ImageIO TIFF plugin (ImageIO, 8233239)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-14621
Title: OpenJDK: XML validation manipulation due to incomplete application of the use-grammar-pool-only feature (JAXP, 8242136)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-2767
Title: OpenJDK: Incorrect handling of Certificate messages during TLS handshake (JSSE, 8232581)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-2781
Title: OpenJDK: Re-use of single TLS session for new connections (JSSE, 8234408)
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-2800

```
Title: OpenJDK: CRLF injection into HTTP headers in HttpServer (Lightweight HTTP Server, 8234825)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2830
Title: OpenJDK: Regular expression DoS in Scanner (Concurrency, 8236201)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2422
Title: OpenJDK: memory disclosure in FileChannelImpl (Libraries, 8206290)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2426
Title: OpenJDK: transparent NTLM authentication enabled by default (Networking, 8209094)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2449
Title: Oracle JDK: unspecified vulnerability fixed in 8u201 (Deployment)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2766
Title: OpenJDK: Insufficient permission checks for file:// URLs on Windows (Networking, 8213431)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2786
Title: OpenJDK: Insufficient restriction of privileges in AccessController (Security, 8216381)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2818
Title: OpenJDK: Non-constant time comparison in ChaCha20Cipher (Security, 8221344)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-2842
Title: OpenJDK: Missing array bounds check in crypto providers (JCE, 8223511)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14573
Title: OpenJDK: Incomplete interface type checks in Graal compiler (Hotspot, 8236867)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14577
Title: OpenJDK: HostnameChecker does not ensure X.509 certificate names are in normalized form (JSSE, 8237592)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14581
Title: OpenJDK: Information disclosure in color management (2D, 8238002)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2754
Title: OpenJDK: Misplaced regular expression syntax error check in RegExpScanner (Scripting, 8223898)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-2755
Title: OpenJDK: Incorrect handling of empty string nodes in regular expression Parser (Scripting, 8223904)
Peso: 1 - Monitorare la vulnerabilità
```

```
------------------
VulnerabilityID: CVE-2020-2756
Title: OpenJDK: Incorrect handling of references to uninitialized class descriptors during deserialization (Serialization,
8224541)
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-2757
Title: OpenJDK: Uncaught InstantiationError exception in ObjectStreamClass (Serialization, 8224549)
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-2773
Title: OpenJDK: Unexpected exceptions raised by DOMKeyInfoFactory and DOMXMLSignatureFactory (Security,
8231415)
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-2778
Title: OpenJDK: Incomplete enforcement of algorithm restrictions for TLS (JSSE, 8232424)
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-12243
Title: openldap: denial of service via nested boolean expressions in LDAP search filters
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-25692
Title: openldap: NULL pointer dereference for unauthenticated packet in slapd
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36221
Title: openldap: Integer underflow in serialNumberAndIssuerCheck in schema_init.c
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36222
Title: openldap: Assertion failure in slapd in the saslAuthzTo validation
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36223
Title: openldap: Out-of-bounds read in Values Return Filter
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36224
Title: openldap: Invalid pointer free in the saslAuthzTo processing
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36225
Title: openldap: Double free in the saslAuthzTo processing
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36226
Title: openldap: Denial of service via length miscalculation in slap_parse_user
Peso: 1 - Monitorare la vulnerabilità
------------------
VulnerabilityID: CVE-2020-36227
Title: openldap: Infinite loop in slapd with the cancel_extop Cancel operation
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2020-36228
Title: openldap: Integer underflow in issuerAndThisUpdateCheck in schema_init.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-36229
Title: openldap: Type confusion in ad_keystring in ad.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-36230
Title: openldap: Assertion failure in ber_next_element in decode.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-27212
Title: openldap: Assertion failure in slapd in the issuerAndThisUpdateCheck function
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23840
Title: openssl: integer overflow in CipherUpdate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3712
Title: openssl: Read buffer overruns processing ASN.1 strings
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-0778
Title: openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-0734
Title: openssl: timing side channel attack in the DSA signature algorithm
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-0735
Title: openssl: timing side channel attack in the ECDSA signature generation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-5407
Title: openssl: Side-channel vulnerability on SMT/Hyper-Threading architectures (PortSmash)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1547
Title: openssl: side-channel weak encryption vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1551
Title: openssl: Integer overflow in RSAZ modular exponentiation on x86_64
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1971
Title: openssl: EDIPARTYNAME NULL pointer de-reference
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23841
```

```
Title: openssl: NULL pointer dereference in X509_issuer_and_serial_hash()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-4160
Title: openssl: Carry propagation bug in the MIPS32 and MIPS64 squaring procedure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1563
Title: openssl: information disclosure in PKCS7_dataDecode and CMS_decrypt_set1_pkey
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1968
Title: openssl: Information exposure when DH secret are reused across multiple TLS connections
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23839
Title: openssl: incorrect SSLv2 rollback protection
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23840
Title: openssl: integer overflow in CipherUpdate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3712
Title: openssl: Read buffer overruns processing ASN.1 strings
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-0778
Title: openssl: Infinite loop in BN_mod_sqrt() reachable when parsing certificates
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-0734
Title: openssl: timing side channel attack in the DSA signature algorithm
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-0735
Title: openssl: timing side channel attack in the ECDSA signature generation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-5407
Title: openssl: Side-channel vulnerability on SMT/Hyper-Threading architectures (PortSmash)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1547
Title: openssl: side-channel weak encryption vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1551
Title: openssl: Integer overflow in RSAZ modular exponentiation on x86_64
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1971
Title: openssl: EDIPARTYNAME NULL pointer de-reference
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2021-23841
Title: openssl: NULL pointer dereference in X509_issuer_and_serial_hash()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-4160
Title: openssl: Carry propagation bug in the MIPS32 and MIPS64 squaring procedure
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-1563
Title: openssl: information disclosure in PKCS7_dataDecode and CMS_decrypt_set1_pkey
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-1968
Title: openssl: Information exposure when DH secret are reused across multiple TLS connections
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-23839
Title: openssl: incorrect SSLv2 rollback protection
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-16231
Title: pcre: self-recursive call in match() in pcre_exec.c leads to denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-14155
Title: pcre: Integer overflow when parsing callout numeric arguments
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-10543
Title: perl: heap-based buffer overflow in regular expression compiler leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-10878
Title: perl: corruption of intermediate language state of compiled regular expression due to integer overflow leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-12723
Title: perl: corruption of intermediate language state of compiled regular expression due to recursive S_study_chunk() calls leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-35457
Title: GNOME GLib before 2.65.3 has an integer overflow, that might lead to a ...
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-27218
Title: glib: integer overflow in g_byte_array_new_take function when called with a buffer of 4GB or more on a 64-bit platform
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1122
Title: procps-ng, procps: Local privilege escalation in top
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2018-1123
Title: procps-ng, procps: denial of service in ps via mmap buffer overflow
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1124
Title: procps-ng, procps: Integer overflows leading to heap overflow in file2strvec
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1125
Title: procps-ng, procps: stack buffer overflow in pgrep
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2015-20107
Title: python: mailcap: findmatch() function does not sanitize the second argument
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1060
Title: python: DOS via regular expression catastrophic backtracking in apop() method in pop3lib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1061
Title: python: DOS via regular expression backtracking in difflib.IS_LINE_JUNK method in difflib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-14647
Title: python: Missing salt initialization in _elementtree.c module
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16056
Title: python: email.utils.parseaddr wrongly parses email addresses
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17514
Title: python: potentially misleading information about whether sorting in library/glob.html
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20907
Title: python: infinite loop in the tarfile module via crafted TAR archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5010
Title: python: NULL pointer dereference using a specially crafted X509 certificate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9674
Title: python: Nested zip file (Zip bomb) vulnerability in Lib/zipfile.py
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20852
Title: python: Cookie domain check returns incorrect results
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16935
```

```
Title: python: XSS vulnerability in the documentation XML-RPC server in server_title field
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18348
Title: python: CRLF injection via the host part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9740
Title: python: CRLF injection via the query part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9947
Title: python: CRLF injection via the path part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8492
Title: python: wrong backtracking in urllib.request.AbstractBasicAuthHandler allows for a ReDoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2015-20107
Title: python: mailcap: findmatch() function does not sanitize the second argument
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1060
Title: python: DOS via regular expression catastrophic backtracking in apop() method in pop3lib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1061
Title: python: DOS via regular expression backtracking in difflib.IS_LINE_JUNK method in difflib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-14647
Title: python: Missing salt initialization in _elementtree.c module
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16056
Title: python: email.utils.parseaddr wrongly parses email addresses
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17514
Title: python: potentially misleading information about whether sorting in library/glob.html
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20907
Title: python: infinite loop in the tarfile module via crafted TAR archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5010
Title: python: NULL pointer dereference using a specially crafted X509 certificate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9674
Title: python: Nested zip file (Zip bomb) vulnerability in Lib/zipfile.py
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2018-20852
Title: python: Cookie domain check returns incorrect results
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16935
Title: python: XSS vulnerability in the documentation XML-RPC server in server_title field
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18348
Title: python: CRLF injection via the host part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9740
Title: python: CRLF injection via the query part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9947
Title: python: CRLF injection via the path part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8492
Title: python: wrong backtracking in urllib.request.AbstractBasicAuthHandler allows for a ReDoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2015-20107
Title: python: mailcap: findmatch() function does not sanitize the second argument
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1060
Title: python: DOS via regular expression catastrophic backtracking in apop() method in pop3lib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-1061
Title: python: DOS via regular expression backtracking in difflib.IS_LINE_JUNK method in difflib
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-14647
Title: python: Missing salt initialization in _elementtree.c module
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16056
Title: python: email.utils.parseaddr wrongly parses email addresses
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-17514
Title: python: potentially misleading information about whether sorting in library/glob.html
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20907
Title: python: infinite loop in the tarfile module via crafted TAR archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-5010
```

```
Title: python: NULL pointer dereference using a specially crafted X509 certificate
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9674
Title: python: Nested zip file (Zip bomb) vulnerability in Lib/zipfile.py
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20852
Title: python: Cookie domain check returns incorrect results
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16935
Title: python: XSS vulnerability in the documentation XML-RPC server in server_title field
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-18348
Title: python: CRLF injection via the host part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9740
Title: python: CRLF injection via the query part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9947
Title: python: CRLF injection via the path part of the url passed to urlopen()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-8492
Title: python: wrong backtracking in urllib.request.AbstractBasicAuthHandler allows for a ReDoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-7500
Title: rpm: Following symlinks to directories when installing packages allows privilege escalation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20271
Title: rpm: Signature checks bypass via corrupted rpm package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20266
Title: rpm: missing length checks in hdrblobInit()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3421
Title: rpm: unsigned signature header leads to string injection into an rpm database
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3521
Title: rpm: RPM does not require subkeys to have a valid binding signature
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-7500
Title: rpm: Following symlinks to directories when installing packages allows privilege escalation
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2021-20271
Title: rpm: Signature checks bypass via corrupted rpm package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20266
Title: rpm: missing length checks in hdrblobInit()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3421
Title: rpm: unsigned signature header leads to string injection into an rpm database
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3521
Title: rpm: RPM does not require subkeys to have a valid binding signature
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-7500
Title: rpm: Following symlinks to directories when installing packages allows privilege escalation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20271
Title: rpm: Signature checks bypass via corrupted rpm package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20266
Title: rpm: missing length checks in hdrblobInit()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3421
Title: rpm: unsigned signature header leads to string injection into an rpm database
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3521
Title: rpm: RPM does not require subkeys to have a valid binding signature
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-7500
Title: rpm: Following symlinks to directories when installing packages allows privilege escalation
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20271
Title: rpm: Signature checks bypass via corrupted rpm package
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-20266
Title: rpm: missing length checks in hdrblobInit()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3421
Title: rpm: unsigned signature header leads to string injection into an rpm database
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3521
```

```
Title: rpm: RPM does not require subkeys to have a valid binding signature
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20346
Title: sqlite: Multiple flaws in sqlite which can be triggered via corrupted internal databases (Magellan)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8740
Title: sqlite: NULL pointer dereference with databases with schema corrupted with CREATE TABLE AS allows for denial
of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19244
Title: sqlite: allows a crash if a sub-select uses both DISTINCT and window functions and also has certain ORDER BY
usage
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19603
Title: sqlite: mishandling of certain SELECT statements with non-existent VIEW can lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19880
Title: sqlite: invalid pointer dereference in exprListAppendList in window.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19923
Title: sqlite: mishandling of certain uses of SELECT DISTINCT involving a LEFT JOIN in flattenSubquery in select.c
leads to a NULL pointer dereference
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19925
Title: sqlite: zipfileUpdate in ext/misc/zipfile.c mishandles a NULL pathname during an update of a ZIP archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19926
Title: sqlite: error mishandling because of incomplete fix of CVE-2019-19880
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19959
Title: sqlite: mishandles certain uses of INSERT INTO in situations involving embedded '\0' characters in filenames
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20218
Title: sqlite: selectExpander in select.c proceeds with WITH stack unwinding even after a parsing error
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9936
Title: sqlite: heap-based buffer over-read in function fts5HashEntrySort in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9937
Title: sqlite: null-pointer dereference in function fts5ChunkIterate in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2020-11655
Title: sqlite: malformed window-function query leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13630
Title: sqlite: Use-after-free in fts3EvalNextRow in ext/fts3/fts3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-9327
Title: sqlite: NULL pointer dereference and segmentation fault because of generated column optimizations
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16168
Title: sqlite: Division by zero in whereLoopAddBtreeIndex in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19242
Title: sqlite: SQL injection in sqlite3ExprCodeTarget in expr.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19645
Title: sqlite: infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13434
Title: sqlite: integer overflow in sqlite3_str_vappendf function in printf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13435
Title: sqlite: NULL pointer dereference in sqlite3ExprCodeTarget()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13631
Title: sqlite: Virtual table can be renamed into the name of one of its shadow tables
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13632
Title: sqlite: NULL pointer dereference in ext/fts3/fts3_snippet.c via a crafted matchinfo() query
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-15358
Title: sqlite: heap-based buffer overflow in multiSelectOrderBy due to mishandling of query-flattener optimization in select.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20346
Title: sqlite: Multiple flaws in sqlite which can be triggered via corrupted internal databases (Magellan)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8740
Title: sqlite: NULL pointer dereference with databases with schema corrupted with CREATE TABLE AS allows for denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2019-19244
Title: sqlite: allows a crash if a sub-select uses both DISTINCT and window functions and also has certain ORDER BY usage
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19603
Title: sqlite: mishandling of certain SELECT statements with non-existent VIEW can lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19880
Title: sqlite: invalid pointer dereference in exprListAppendList in window.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19923
Title: sqlite: mishandling of certain uses of SELECT DISTINCT involving a LEFT JOIN in flattenSubquery in select.c leads to a NULL pointer dereference
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19925
Title: sqlite: zipfileUpdate in ext/misc/zipfile.c mishandles a NULL pathname during an update of a ZIP archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19926
Title: sqlite: error mishandling because of incomplete fix of CVE-2019-19880
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19959
Title: sqlite: mishandles certain uses of INSERT INTO in situations involving embedded '\0' characters in filenames
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20218
Title: sqlite: selectExpander in select.c proceeds with WITH stack unwinding even after a parsing error
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9936
Title: sqlite: heap-based buffer over-read in function fts5HashEntrySort in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9937
Title: sqlite: null-pointer dereference in function fts5ChunkIterate in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-11655
Title: sqlite: malformed window-function query leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13630
Title: sqlite: Use-after-free in fts3EvalNextRow in ext/fts3/fts3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-9327
Title: sqlite: NULL pointer dereference and segmentation fault because of generated column optimizations
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

```
VulnerabilityID: CVE-2019-16168
Title: sqlite: Division by zero in whereLoopAddBtreeIndex in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19242
Title: sqlite: SQL injection in sqlite3ExprCodeTarget in expr.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19645
Title: sqlite: infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13434
Title: sqlite: integer overflow in sqlite3_str_vappendf function in printf.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13435
Title: sqlite: NULL pointer dereference in sqlite3ExprCodeTarget()
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13631
Title: sqlite: Virtual table can be renamed into the name of one of its shadow tables
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13632
Title: sqlite: NULL pointer dereference in ext/fts3/fts3_snippet.c via a crafted matchinfo() query
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-15358
Title: sqlite: heap-based buffer overflow in multiSelectOrderBy due to mishandling of query-flattener optimization in select.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-20346
Title: sqlite: Multiple flaws in sqlite which can be triggered via corrupted internal databases (Magellan)
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-8740
Title: sqlite: NULL pointer dereference with databases with schema corrupted with CREATE TABLE AS allows for denial of service
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19244
Title: sqlite: allows a crash if a sub-select uses both DISTINCT and window functions and also has certain ORDER BY usage
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19603
Title: sqlite: mishandling of certain SELECT statements with non-existent VIEW can lead to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19880
Title: sqlite: invalid pointer dereference in exprListAppendList in window.c
Peso: 1 - Monitorare la vulnerabilità
```

```
-------------------
VulnerabilityID: CVE-2019-19923
Title: sqlite: mishandling of certain uses of SELECT DISTINCT involving a LEFT JOIN in flattenSubquery in select.c
leads to a NULL pointer dereference
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19925
Title: sqlite: zipfileUpdate in ext/misc/zipfile.c mishandles a NULL pathname during an update of a ZIP archive
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19926
Title: sqlite: error mishandling because of incomplete fix of CVE-2019-19880
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19959
Title: sqlite: mishandles certain uses of INSERT INTO in situations involving embedded '\0' characters in filenames
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20218
Title: sqlite: selectExpander in select.c proceeds with WITH stack unwinding even after a parsing error
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9936
Title: sqlite: heap-based buffer over-read in function fts5HashEntrySort in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-9937
Title: sqlite: null-pointer dereference in function fts5ChunkIterate in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-11655
Title: sqlite: malformed window-function query leads to DoS
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13630
Title: sqlite: Use-after-free in fts3EvalNextRow in ext/fts3/fts3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-9327
Title: sqlite: NULL pointer dereference and segmentation fault because of generated column optimizations
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-16168
Title: sqlite: Division by zero in whereLoopAddBtreeIndex in sqlite3.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19242
Title: sqlite: SQL injection in sqlite3ExprCodeTarget in expr.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-19645
Title: sqlite: infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements
Peso: 1 - Monitorare la vulnerabilità
-------------------
```

VulnerabilityID: CVE-2020-13434
Title: sqlite: integer overflow in sqlite3_str_vappendf function in printf.c
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-13435
Title: sqlite: NULL pointer dereference in sqlite3ExprCodeTarget()
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-13631
Title: sqlite: Virtual table can be renamed into the name of one of its shadow tables
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-13632
Title: sqlite: NULL pointer dereference in ext/fts3/fts3_snippet.c via a crafted matchinfo() query
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-15358
Title: sqlite: heap-based buffer overflow in multiSelectOrderBy due to mishandling of query-flattener optimization in select.c
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-15686
Title: systemd: line splitting via fgets() allows for state injection during daemon-reexec
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-15688
Title: systemd: Out-of-bounds heap write in systemd-networkd dhcpv6 option handling
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-16864
Title: systemd: stack overflow when calling syslog from a command with long cmdline
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-16865
Title: systemd: stack overflow when receiving many journald entries
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2018-6954
Title: systemd: Mishandled symlinks in systemd-tmpfiles allows local users to obtain ownership of arbitrary files
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-3842
Title: systemd: Spoofing of XDG_SEAT allows for actions to be checked against "allow_active" instead of "allow_any"
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-3843
Title: systemd: services with DynamicUser can create SUID/SGID binaries
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2019-3844
Title: systemd: services with DynamicUser can get new privileges and create SGID binaries
Peso: 1 - Monitorare la vulnerabilità

VulnerabilityID: CVE-2020-1712

```
Title: systemd: use-after-free when asynchronous polkit queries are performed
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-6454
Title: systemd: Insufficient input validation in bus_process_object() resulting in PID 1 crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13529
Title: systemd: DHCP FORCERENEW authentication not implemented can cause a system running the DHCP client to have its network reconfigured
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2020-13776
Title: systemd: Mishandles numerical usernames beginning with decimal digits or 0x followed by hexadecimal digits
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-33910
Title: systemd: uncontrolled allocation on the stack in function unit_name_path_escape leads to crash
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-16866
Title: systemd: out-of-bounds read when parsing a crafted syslog message
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2019-20386
Title: systemd: memory leak in button_open() in login/logind-button.c when udev events are received
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7738
Title: util-linux: Shell command injection in unescaped bash-completed mount point names
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-2616
Title: util-linux: Sending SIGKILL to other processes with root privileges via su
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-37600
Title: util-linux: integer overflow can lead to buffer overflow in get_sem_elements() in sys-utils/ipcutils.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-0563
Title: util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7738
Title: util-linux: Shell command injection in unescaped bash-completed mount point names
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-2616
Title: util-linux: Sending SIGKILL to other processes with root privileges via su
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-37600
Title: util-linux: integer overflow can lead to buffer overflow in get_sem_elements() in sys-utils/ipcutils.c
```

```
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-0563
Title: util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-7738
Title: util-linux: Shell command injection in unescaped bash-completed mount point names
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2017-2616
Title: util-linux: Sending SIGKILL to other processes with root privileges via su
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-37600
Title: util-linux: integer overflow can lead to buffer overflow in get_sem_elements() in sys-utils/ipcutils.c
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-0563
Title: util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled with libreadline
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-1271
Title: gzip: arbitrary-file-write vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2022-1271
Title: gzip: arbitrary-file-write vulnerability
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-25032
Title: zlib: A flaw found in zlib when compressing (not decompressing) certain inputs
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2018-25032
Title: zlib: A flaw found in zlib when compressing (not decompressing) certain inputs
Peso: 1 - Monitorare la vulnerabilità
-------------------
VulnerabilityID: CVE-2021-3487
Title: binutils: Excessive debug section size can cause excessive memory consumption in bfd's dwarf2.c read_section()
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2022-22623
Title:
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2022-22623
Title:
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2022-22623
Title:
Peso: 0 - Situazione sotto controllo
-------------------
```

```
VulnerabilityID: CVE-2016-10739
Title: glibc: getaddrinfo should reject IP addresses with trailing characters
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2016-10739
Title: glibc: getaddrinfo should reject IP addresses with trailing characters
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2021-20223
Title:
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2021-20223
Title:
Peso: 0 - Situazione sotto controllo
-------------------
VulnerabilityID: CVE-2021-20223
Title:
Peso: 0 - Situazione sotto controllo
-------------------
```