Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

Attack Vector: Network, Severity: Critical

CVE-2019-9169	
Vers: 2.28-127.el8	Fix: 0:2.28-151.el8
Name: glibc-minimal-langpack Namespace: centos:8 Description: The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly. Security Fix(es): * glibc: buffer over-read in iconv when processing invalid multi-byte input sequences in the EUC-KR encoding (CVE-2019-25013) * glibc: regular-expression match via proceed_next_node in posix/regexec.c leads to heap-based buffer over-read (CVE-2019-9169) * glibc: assertion failure in ISO-2022-JP-3 gconv module related to combining characters (CVE-2021-3326) * glibc: iconv program can hang when invoked with the -c option (CVE-2016-10228) * glibc: iconv when processing invalid multi-byte input sequences fails to advance the input state, which could result in an infinite loop (CVE-2020-27618) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-27619	
Vers: 3.6.8-31.el8	Fix: 0:3.6.8-37.el8
Name: python3-libs Namespace: centos:8 Description: Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Security Fix(es): * python: CRLF injection via HTTP request method in httplib/http.client (CVE-2020-26116) * python: Unsafe use of eval() on data retrieved via HTTP in the test suite (CVE-2020-27619) * python: Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c (CVE-2021-3177) * python: Web cache poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a semicolon in query parameters (CVE-2021-23336) For more details	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.

CVE-2021-3177	
Vers: 3.6.8-31.el8	Fix: 0:3.6.8-37.el8
Name: python3-libs Namespace: centos:8 Description: Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Security Fix(es): * python: CRLF injection via HTTP request method in httplib/http.client (CVE-2020-26116) * python: Unsafe use of eval() on data retrieved via HTTP in the test suite (CVE-2020-27619) * python: Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c (CVE-2021-3177) * python: Web cache poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a semicolon in query parameters (CVE-2021-23336) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2021-3520	
Vers: 1.8.3-2.el8	Fix: 0:1.8.3-3.el8_4
Name: lz4-libs Namespace: centos:8 Description: The lz4 packages provide support for LZ4, a very fast, lossless compression algorithm that provides compression speeds of 400 MB/s per core and scales with multicore CPUs. It also features an extremely fast decoder that reaches speeds of multiple GB/s per core and typically reaches RAM speed limits on multicore systems. Security Fix(es): * lz4: memory corruption due to an integer overflow bug caused by memmove argument (CVE-2021-3520) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

Attack Vector: Network, Severity: High

CVE-2017-14502	
Vers: 3.3.2-9.el8	Fix: 0:3.3.3-1.el8
Name: libarchive Namespace: centos:8 Description: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2019-13012	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-13543	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.

CVE-2020-13584	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-1971	
Vers: 1:1.1.1g-11.el8	Fix: 1:1.1.1g-12.el8_3
Name: openssl-libs Namespace: centos:8 Description: OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library. Security Fix(es): * openssl: EDIPARTYNAME NULL pointer de-reference (CVE-2020-1971) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

other related information, refer to the CVE page(s) listed in the References section. Bug Fix(es): * Reject certificates with explicit EC parameters in strict mode (BZ#1891541) * Add FIPS selftest for HKDF, SSKDF, SSHKDF, and TLS12PRF; add DH_compute_key KAT to DH selftest (BZ#1891542)

CVE-2020-24659	
Vers: 3.6.14-6.el8	Fix: 0:3.6.14-7.el8_3
Name: gnutls Namespace: centos:8 Description: The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic algorithms and protocols such as SSL, TLS, and DTLS. Security Fix(es): * gnutls: Heap buffer overflow in handshake with no_renegotiation alert sent (CVE-2020-24659) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Bug Fix(es): * gnutls: Add self-tests for implemented KDF algorithms and CMAC (BZ#1903037)	

CVE-2020-26116	
Vers: 3.6.8-31.el8	Fix: 0:3.6.8-37.el8
Name: python3-libs Namespace: centos:8 Description: Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Security Fix(es): * python: CRLF injection via HTTP request method in httplib/http.client (CVE-2020-26116) * python: Unsafe use of eval() on data retrieved via HTTP in the test suite (CVE-2020-27619) * python: Stack-based buffer overflow in PyCArg_repr in _ctypes/callproc.c (CVE-2021-3177) * python: Web cache poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a semicolon in query parameters (CVE-2021-23336) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-28196

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

Vers: 1.18.2-5.el8	Fix: 0:1.18.2-8.el8
Name: krb5-libs Namespace: centos:8 Description: Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center (KDC). Security Fix(es): * krb5: unbounded recursion via an ASN.1-encoded Kerberos message in lib/krb5/asn.1/asn1_encode.c may lead to DoS (CVE-2020-28196) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-29361	
Vers: 0.23.14-5.el8_0	Fix: 0:0.23.22-1.el8
Name: p11-kit-trust Namespace: centos:8 Description: The p11-kit packages provide a mechanism to manage PKCS#11 modules. The p11-kit-trust subpackage includes a PKCS#11 trust module that provides certificate anchors and black lists based on configuration files. The following packages have been upgraded to a later upstream version: p11-kit (0.23.22). (BZ#1887853) Security Fix(es): * p11-kit: integer overflow when allocating memory for arrays or attributes and object identifiers (CVE-2020-29361) * p11-kit: out-of-bounds read in p11_rpc_buffer_get_byte_array function in rpc-message.c (CVE-2020-29362) * p11-kit: out-of-bounds write in p11_rpc_buffer_get_byte_array_value function in rpc-message.c (CVE-2020-29363) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-29363	
Vers: 0.23.14-5.el8_0	Fix: 0:0.23.22-1.el8
Name: p11-kit-trust Namespace: centos:8 Description: The p11-kit packages provide a mechanism to manage PKCS#11 modules. The	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

p11-kit-trust subpackage includes a PKCS#11 trust module that provides certificate anchors and black lists based on configuration files. The following packages have been upgraded to a later upstream version: p11-kit (0.23.22). (BZ#1887853) Security Fix(es): * p11-kit: integer overflow when allocating memory for arrays or attributes and object identifiers (CVE-2020-29361) * p11-kit: out-of-bounds read in p11_rpc_buffer_get_byte_array function in rpc-message.c (CVE-2020-29362) * p11-kit: out-of-bounds write in p11_rpc_buffer_get_byte_array_value function in rpc-message.c (CVE-2020-29363) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.

CVE-2020-8231	
Vers: 7.61.1-14.el8	Fix: 0:7.61.1-18.el8
Name: libcurl-minimal Namespace: centos:8 Description: The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Security Fix(es): * curl: FTP PASV command response can cause curl to connect to arbitrary host (CVE-2020-8284) * curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used (CVE-2020-8285) * curl: Inferior OCSP verification (CVE-2020-8286) * curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set (CVE-2020-8231) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-8285	
Vers: 7.61.1-14.el8	Fix: 0:7.61.1-18.el8
Name: libcurl-minimal Namespace: centos:8 Description: The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Security Fix(es): * curl: FTP PASV command response can cause curl to connect to arbitrary host (CVE-2020-8284) * curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

used (CVE-2020-8285) * curl: Inferior OCSP verification (CVE-2020-8286) * curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set (CVE-2020-8231) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.

CVE-2020-8286	
Vers: 7.61.1-14.el8	Fix: 0:7.61.1-18.el8
Name: libcurl-minimal Namespace: centos:8 Description: The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Security Fix(es): * curl: FTP PASV command response can cause curl to connect to arbitrary host (CVE-2020-8284) * curl: Malicious FTP server can trigger stack overflow when CURLOPT_CHUNK_BGN_FUNCTION is used (CVE-2020-8285) * curl: Inferior OCSP verification (CVE-2020-8286) * curl: Expired pointer dereference via multi API with CURLOPT_CONNECT_ONLY option set (CVE-2020-8231) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-8625	
Vers: 32:9.11.20-5.el8	Fix: 32:9.11.20-5.el8_3.1
Name: bind-export-libs Namespace: centos:8 Description: The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly. Security Fix(es): * bind: Buffer overflow in the SPNEGO implementation affecting GSSAPI security policy negotiation (CVE-2020-8625) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

CVE-2020-9948	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2020-9951	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

CVE-2020-9983	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-9.el8
Name: glib2 Namespace: centos:8 Description: GNOME is the default desktop environment of Red Hat Enterprise Linux. The following packages have been upgraded to a later upstream version: accountsservice (0.6.55), webkit2gtk3 (2.30.4). (BZ#1846376, BZ#1883304) Security Fix(es): * webkitgtk: type confusion may lead to arbitrary code execution (CVE-2020-9948) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-9951) * webkitgtk: out-of-bounds write may lead to code execution (CVE-2020-9983) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13543) * webkitgtk: use-after-free may lead to arbitrary code execution (CVE-2020-13584) * glib2: insecure permissions for files and directories (CVE-2019-13012) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2021-20271	
Vers: 4.14.3-4.el8	Fix: 0:4.14.3-14.el8_4
Name: rpm-libs Namespace: centos:8 Description: The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Security Fix(es): * rpm: Signature checks bypass via corrupted rpm package (CVE-2021-20271) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

CVE-2021-20305	
Vers: 3.4.1-2.el8	Fix: 0:3.4.1-4.el8_3
Name: nettle Namespace: centos:8 Description: The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic algorithms and protocols such as SSL, TLS, and DTLS. Nettle is a cryptographic library that is designed to fit easily in almost any context: In crypto toolkits for	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

object-oriented languages, such as C++, Python, or Pike, in applications like LSH or GNUPG, or even in kernel space. Security Fix(es): * nettle: Out of bounds memory access in signature verification (CVE-2021-20305) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

CVE-2021-25215	
Vers: 32:9.11.20-5.el8	Fix: 32:9.11.26-4.el8_4
Name: bind-export-libs Namespace: centos:8 Description: The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly. Security Fix(es): * bind: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve itself (CVE-2021-25215) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

CVE-2021-27218	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-10.el8_4.1
Name: glib2 Namespace: centos:8 Description: GLib provides the core application building blocks for libraries and applications written in C. It provides the core object system used in GNOME, the main loop implementation, and a large set of utility functions for strings and common data structures. Security Fix(es): * glib: integer overflow in g_byte_array_new_take function when called with a buffer of 4GB or more on a 64-bit platform (CVE-2021-27218) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

CVE-2021-27219	
Vers: 2.56.4-8.el8	Fix: 0:2.56.4-10.el8_4
Name: glib2 Namespace: centos:8	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

Description: GLib provides the core application building blocks for libraries and applications written in C. It provides the core object system used in GNOME, the main loop implementation, and a large set of utility functions for strings and common data structures. Security Fix(es): * glib: integer overflow in g_bytes_new function on 64-bit platforms due to an implicit cast from 64 bits to 32 bits (CVE-2021-27219) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Bug Fix(es): * Refcounting issue causes crashes and slow workarounds (BZ#1953553)

CVE-2021-3326	
Vers: 2.28-127.el8	Fix: 0:2.28-151.el8
Name: glibc-minimal-langpack Namespace: centos:8 Description: The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly. Security Fix(es): * glibc: buffer over-read in iconv when processing invalid multi-byte input sequences in the EUC-KR encoding (CVE-2019-25013) * glibc: regular-expression match via proceed_next_node in posix/regexec.c leads to heap-based buffer over-read (CVE-2019-9169) * glibc: assertion failure in ISO-2022-JP-3 gconv module related to combining characters (CVE-2021-3326) * glibc: iconv program can hang when invoked with the -c option (CVE-2016-10228) * glibc: iconv when processing invalid multi-byte input sequences fails to advance the input state, which could result in an infinite loop (CVE-2020-27618) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 8.4 Release Notes linked from the References section.	

CVE-2021-3449	
Vers: 1:1.1.1g-11.el8	Fix: 1:1.1.1g-15.el8_3
Name: openssl-libs Namespace: centos:8 Description: OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library. Security Fix(es): * openssl: NULL pointer dereference in signature_algorithms processing	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

(CVE-2021-3449) * openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT (CVE-2021-3450) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

CVE-2021-3450	
Vers: 1:1.1.1g-11.el8	Fix: 1:1.1.1g-15.el8_3
Name: openssl-libs Namespace: centos:8 Description: OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library. Security Fix(es): * openssl: NULL pointer dereference in signature_algorithms processing (CVE-2021-3449) * openssl: CA certificate check bypass with X509_V_FLAG_X509_STRICT (CVE-2021-3450) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

CVE-2021-3516	
Vers: 2.9.7-8.el8	Fix: 0:2.9.7-9.el8_4.2
Name: libxml2 Namespace: centos:8 Description: The libxml2 library is a development toolbox providing the implementation of various XML standards. Security Fix(es): * libxml2: Use-after-free in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3516) * libxml2: Heap-based buffer overflow in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3517) * libxml2: Use-after-free in xmlXIncludeDoProcess() in xinclude.c (CVE-2021-3518) * libxml2: NULL pointer dereference when post-validating mixed content parsed in recovery mode (CVE-2021-3537) * libxml2: Exponential entity expansion attack bypasses all existing protection mechanisms (CVE-2021-3541) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

CVE-2021-3517	
Vers: 2.9.7-8.el8	Fix: 0:2.9.7-9.el8_4.2
Name: libxml2	

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

Namespace: centos:8 Description: The libxml2 library is a development toolbox providing the implementation of various XML standards. Security Fix(es): * libxml2: Use-after-free in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3516) * libxml2: Heap-based buffer overflow in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3517) * libxml2: Use-after-free in xmlXIncludeDoProcess() in xinclude.c (CVE-2021-3518) * libxml2: NULL pointer dereference when post-validating mixed content parsed in recovery mode (CVE-2021-3537) * libxml2: Exponential entity expansion attack bypasses all existing protection mechanisms (CVE-2021-3541) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

CVE-2021-3518	
Vers: 2.9.7-8.el8	Fix: 0:2.9.7-9.el8_4.2
Name: libxml2 Namespace: centos:8 Description: The libxml2 library is a development toolbox providing the implementation of various XML standards. Security Fix(es): * libxml2: Use-after-free in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3516) * libxml2: Heap-based buffer overflow in xmlEncodeEntitiesInternal() in entities.c (CVE-2021-3517) * libxml2: Use-after-free in xmlXIncludeDoProcess() in xinclude.c (CVE-2021-3518) * libxml2: NULL pointer dereference when post-validating mixed content parsed in recovery mode (CVE-2021-3537) * libxml2: Exponential entity expansion attack bypasses all existing protection mechanisms (CVE-2021-3541) For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.	

Additional Findings

CVE-2016-10228	AV: network	Severity: medium
CVE-2019-14866	AV: local	Severity: high
CVE-2019-18276	AV: local	Severity: high
CVE-2019-25013	AV: network	Severity: medium
CVE-2019-3842	AV: local	Severity: high
CVE-2020-13434	AV: local	Severity: medium

Scan Report: centos:latest

Scan ID: 4905f10b-c32d-4728-9931-f7c0667937b6
Scan requested at: 2021-08-18T18:31:29Z
Database time: 2021-08-18T10:05:22Z
Vulnerabilities: defcon1 - 0, critical - 8, high - 53, medium - 24

CVE-2020-13776	AV: local	Severity: medium
CVE-2020-15358	AV: local	Severity: medium
CVE-2020-24977	AV: network	Severity: medium
CVE-2020-27618	AV: local	Severity: medium
CVE-2020-29362	AV: network	Severity: medium
CVE-2020-8284	AV: network	Severity: medium
CVE-2021-23336	AV: network	Severity: medium
CVE-2021-25217	AV: local	Severity: high
CVE-2021-33910	AV: local	Severity: high
CVE-2021-3537	AV: network	Severity: medium
CVE-2021-3541	AV: network	Severity: medium