SSA-389290: Third-Party Component Vulnerabilities in SINEC INS

Publication Date:	2022-03-08
Last Update:	2022-03-08
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

71 vulnerabilities in third-party components as Node.js, cURL, SQLite, CivetWeb and DNS(ISC BIND) could allow an attacker to interfere with the affected product in various ways.

Siemens has released an update for SINEC INS and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC INS: All versions < V1.0.1.1	Update to V1.0.1.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109806100/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SINEC INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial networks.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2019-19242

SQLite 3.30.1 mishandles pExpr->y.pTab, as demonstrated by the TK_COLUMN case in sqlite3ExprCodeTarget in expr.c.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2019-19244

Select in select.c in SQLite 3.30.1 allows a crash if a sub-select uses both DISTINCT and window functions, and also has certain ORDER BY usage.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2019-19317

lookupName in resolve.c in SQLite 3.30.1 omits bits from the colUsed bitmask in the case of a generated column, which allows attackers to cause a denial of service or possibly have unspecified other impact.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-681: Incorrect Conversion between Numeric Types

Vulnerability CVE-2019-19603

SQLite 3.30.1 mishandles certain SELECT statements with a nonexistent VIEW, leading to an application crash.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2019-19645

alter.c in SQLite through 3.30.1 allows attackers to trigger infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-674: Uncontrolled Recursion

Vulnerability CVE-2019-19646

pragma.c in SQLite through 3.30.1 mishandles NOT NULL in an integrity_check PRAGMA command in certain cases of generated columns.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2019-19880

exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2019-19923

flattenSubquery in select.c in SQLite 3.30.1 mishandles certain uses of SELECT DISTINCT involving a LEFT JOIN in which the right-hand side is a view. This can cause a NULL pointer dereference (or incorrect results).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2019-19924

SQLite 3.30.1 mishandles certain parser-tree rewriting, related to expr.c, vdbeaux.c, and window.c. This is caused by incorrect sqlite3WindowRewrite() error handling.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

Vulnerability CVE-2019-19925

zipfileUpdate in ext/misc/zipfile.c in SQLite 3.30.1 mishandles a NULL pathname during an update of a ZIP archive.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2019-19926

multiSelect in select.c in SQLite 3.30.1 mishandles certain errors during parsing, as demonstrated by errors from sqlite3WindowRewrite() calls. NOTE: this vulnerability exists because of an incomplete fix for CVE-2019-19880.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-1971

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-7774

This affects the package y18n before 3.2.2, 4.0.1 and 5.0.5. PoC by po6ix: const y18n = require('y18n')(); y18n.setLocale('**proto**'); y18n.updateLocale({polluted: true}); console.log(polluted); // true

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

Vulnerability CVE-2020-8169

The libcurl library versions 7.62.0 to and including 7.70.0 are vulnerable to an information disclosure vulnerability that can lead to a partial password being leaked over the network and to the DNS server(s).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2020-8177

curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Vulnerability CVE-2020-8231

Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-8265

Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 are vulnerable to a use-after-free bug in its TLS implementation. When writing to a TLS enabled socket, node::StreamBase::Write calls node::TLSWrap::DoWrite with a freshly allocated WriteWrap object as first argument. If the DoWrite method does not return an error, this object is passed back to the caller as part of a StreamWriteResult structure. This may be exploited to corrupt memory leading to a Denial of Service or potentially other exploits.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-8284

A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2020-8285

curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-674: Uncontrolled Recursion

Vulnerability CVE-2020-8286

The libcurl library versions 7.41.0 to and including 7.73.0 are vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response. This vulnerability could allow an attacker to pass a revoked certificate as valid.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2020-8287

Node.js versions before 10.23.1, 12.20.1, 14.15.4, 15.5.1 allow two copies of a header field in an HTTP request (for example, two Transfer-Encoding header fields). In this case, Node.js identifies the first header field and ignores the second. This can lead to HTTP Request Smuggling.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-444: Inconsistent Interpretation of HTTP Requests (‘HTTP Request Smuggling’)

Vulnerability CVE-2020-8625

BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND’s default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting valid values for the tkey-gssapi-keytab or tkey-gssapi-credentialconfiguration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process. However, remote code execution, while unproven, is theoretically possible. Affects: BIND 9.5.0 -> 9.11.27, 9.12.0 -> 9.16.11, and versions BIND 9.11.3-S1 -> 9.11.27-S1 and 9.16.8-S1 -> 9.16.11-S1 of BIND Supported Preview Edition. Also release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2020-9327

In SQLite 3.31.1, isAuxiliaryVtabOperator allows attackers to trigger a NULL pointer dereference and segmentation fault because of generated column optimizations.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-11655

SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-665: Improper Initialization

Vulnerability CVE-2020-11656

In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-13630

ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-13631

SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c and build.c.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2020-13632

ext/fts3/fts3_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference via a crafted matchinfo() query.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-13871

SQLite 3.32.2 has a use-after-free in resetAccumulator in select.c because the parse tree rewrite for window functions is too late.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2020-15358

In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2020-27304

The CivetWeb web library does not validate uploaded filepaths when running on an OS other than Windows, when using the built-in HTTP form-based file upload mechanism, via the mg_handle_form_request API. Web applications that use the file upload form handler, and use parts of the user-controlled filename in the output path, are susceptible to directory traversal

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)

Vulnerability CVE-2021-3449

An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-3450

The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named "purpose" values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2021-3672

A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-3711

In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2021-3712

ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own “d2i” functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the “data” and “length” fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the “data” field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-22876

curl 7.1.1 to and including 7.75.0 is vulnerable to an “Exposure of Private Personal Information to an Unauthorized Actor” by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-22883

Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to a denial of service attack when too many connection attempts with an ‘unknownProtocol’ are established. This leads to a leak of file descriptors. If a file descriptor limit is configured on the system, then the server is unable to accept new connections and prevent the process also from opening, e.g. a file. If no file descriptor limit is configured, then this lead to an excessive memory usage and cause the system to run out of memory.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2021-22884

Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks as the whitelist includes “localhost6”. When “localhost6” is not present in /etc/hosts, it is just an ordinary domain that is resolved via DNS, i.e., over network. If the attacker controls the victim’s DNS server or can spoof its responses, the DNS rebinding protection can be bypassed by using the “localhost6” domain. As long as the attacker uses the “localhost6” domain, they can still apply the attack described in CVE-2018-7160.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-22890

curl 7.63.0 to and including 7.75.0 includes vulnerability that allows a malicious HTTPS proxy to MITM a connection due to bad handling of TLS 1.3 session tickets. When using a HTTPS proxy and TLS 1.3, libcurl can confuse session tickets arriving from the HTTPS proxy but work as if they arrived from the remote server and then wrongly “short-cut” the host handshake. When confusing the tickets, a HTTPS proxy can trick libcurl to use the wrong session ticket resume for the host and thereby circumvent the server TLS certificate check and make a MITM attack to be possible to perform unnoticed. Note that such a malicious HTTPS proxy needs to provide a certificate that curl will accept for the MITMed server for an attack to work - unless curl has been told to ignore the server certificate check.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability CVE-2021-22897

curl 7.61.0 through 7.76.1 suffers from exposure of data element to wrong session due to a mistake in the code for CURLOPT_SSL_CIPHER_LIST when libcurl is built to use the Schannel TLS library. The selected cipher set was stored in a single “static” variable in the library, which has the surprising side-effect that if an application sets up multiple concurrent transfers, the last one that sets the ciphers will accidentally control the set used by all transfers. In a worst-case scenario, this weakens transport security significantly.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2021-22898

curl 7.7 through 7.76.1 suffers from an information disclosure when the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-909: Missing Initialization of Resource

Vulnerability CVE-2021-22901

curl 7.75.0 through 7.76.1 suffers from a use-after-free vulnerability resulting in already freed memory being used when a TLS 1.3 session ticket arrives over a connection. A malicious server can use this in rare unfortunate circumstances to potentially reach remote code execution in the client. When libcurl at run-time sets up support for TLS 1.3 session tickets on a connection using OpenSSL, it stores pointers to the transfer in-memory object for later retrieval when a session ticket arrives. If the connection is used by multiple transfers (like with a reused HTTP/1.1 connection or multiplexed HTTP/2 connection) that first transfer object might be freed before the new session is established on that connection and then the function will access a memory buffer that might be freed. When using that memory, libcurl might even call a function pointer in the object, making it possible for a remote code execution if the server could somehow manage to get crafted memory content into the correct place in memory.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-22918

Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo().

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-22921

Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-22922

When curl is instructed to download content using the metalink feature, thecontents is verified against a hash provided in the metalink XML file.The metalink XML file points out to the client how to get the same contentfrom a set of different URLs, potentially hosted by different servers and theclient can then download the file from one or several of them. In a serial orparallel manner.If one of the servers hosting the contents has been breached and the contentsof the specific file on that server is replaced with a modified payload, curlshould detect this when the hash of the file mismatches after a completeddownload. It should remove the contents and instead try getting the contentsfrom another URL. This is not done, and instead such a hash mismatch is onlymentioned in text and the potentially malicious content is kept in the file ondisk.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-354: Improper Validation of Integrity Check Value

Vulnerability CVE-2021-22923

When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-522: Insufficiently Protected Credentials

Vulnerability CVE-2021-22924

libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse, if one of them matches the setup. Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections. File paths are, or can be, case sensitive on many systems but not all, and can even vary depending on used file systems. The comparison also didn't include the 'issuer cert' which a transfer can set to qualify how to verify the server certificate.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-706: Use of Incorrectly-Resolved Name or Reference

Vulnerability CVE-2021-22925

curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS`in libcurl. This rarely used option is used to send variable=content pairs toTELNET servers.Due to flaw in the option parser for sending `NEW_ENV` variables, libcurlcould be made to pass on uninitialized data from a stack based buffer to theserver. Therefore potentially revealing sensitive internal information to theserver using a clear-text network protocol.This could happen because curl did not call and use sscanf() correctly whenparsing the string provided by the application.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-908: Use of Uninitialized Resource

Vulnerability CVE-2021-22926

libcurl-using applications can ask for a specific client certificate to be used in a transfer. This is done with the `CURLOPT_SSLCERT` option (`--cert` with the command line tool).When libcurl is built to use the macOS native TLS library Secure Transport, an application can ask for the client certificate by name or with a file name - using the same option. If the name exists as a file, it will be used instead of by name.If the appliction runs with a current working directory that is writable by other users (like `/tmp`), a malicious user can create a file name with the same name as the app wants to use by name, and thereby trick the application to use the file based cert instead of the one referred to by name making libcurl send the wrong client certificate in the TLS connection handshake.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2021-22930

Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-22931

Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS, Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-22939

If the Node.js https API was used incorrectly and “undefined” was in passed for the “rejectUnauthorized” parameter, no error was returned and connections to servers with an expired certificate would have been accepted.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2021-22940

Node.js before 16.6.1, 14.17.5, and 12.22.5 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-22945

When sending data to an MQTT server, libcurl <= 7.73.0 and 7.78.0 could in some circumstances erroneously keep a pointer to an already freed memory area and both use that again in a subsequent call to send data and also free it *again*.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2021-22946

A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server (`--ssl-reqd` on the command line or`CURLOPT_USE_SSL` set to `CURLUSESSL_CONTROL` or `CURLUSESSL_ALL` withlibcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response.This flaw would then make curl silently continue its operations **withoutTLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2021-22947

When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgrade to TLS security, the server can respond and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-queue of cached responses but instead continue using and trustingthe responses it got *before* the TLS handshake as if they were authenticated.Using this flaw, it allows a Man-In-The-Middle attacker to first inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data back to the user thinking the attacker's injected data comes from the TLS-protected server.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

Vulnerability CVE-2021-23362

The package hosted-git-info before 3.0.8 are vulnerable to Regular Expression Denial of Service (ReDoS) via regular expression shortcutMatch in the fromUrl function in index.js. The affected regular expression exhibits polynomial worst-case time complexity.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-23840

Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-25214

In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malformed IXFR triggering the flaw described above, the named process will terminate due to a failed assertion the next time the transferred secondary zone is refreshed.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-617: Reachable Assertion

Vulnerability CVE-2021-25215

In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a query for a record triggering the flaw described above, the named process will terminate due to a failed assertion check. The vulnerability affects all currently maintained BIND 9 branches (9.11, 9.11-S, 9.16, 9.16-S, 9.17) as well as all other versions of BIND 9.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-617: Reachable Assertion

Vulnerability CVE-2021-25216

In BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.11.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch, BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting values for the tkey-gssapi-keytab or tkey-gssapi-credential configuration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. For servers that meet these conditions, the ISC SPNEGO implementation is vulnerable to various attacks, depending on the CPU architecture for which BIND was built: For named binaries compiled for 64-bit platforms, this flaw can be used to trigger a buffer over-read, leading to a server crash. For named binaries compiled for 32-bit platforms, this flaw can be used to trigger a server crash due to a buffer overflow and possibly also to achieve remote code execution. We have determined that standard SPNEGO implementations are available in the MIT and Heimdal Kerberos libraries, which support a broad range of operating systems, rendering the ISC implementation unnecessary and obsolete. Therefore, to reduce the attack surface for BIND users, we will be removing the ISC SPNEGO implementation in the April releases of BIND 9.11 and 9.16 (it had already been dropped from BIND 9.17). We would not normally remove something from a stable ESV (Extended Support Version) of BIND, but since system libraries can replace the ISC SPNEGO implementation, we have made an exception in this case for reasons of stability and security.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-617: Reachable Assertion

Vulnerability CVE-2021-25219

In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.18 of the BIND 9.17 development branch, exploitation of broken authoritative servers using a flaw in response processing can cause degradation in BIND resolver performance. The way the lame cache is currently designed makes it possible for its internal data structures to grow almost infinitely, which may cause significant delays in client query processing.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-27290

ssri 5.2.2-8.0.0, fixed in 8.0.1, processes SRIs using a regular expression which is vulnerable to a denial of service. Malicious SRIs could take an extremely long time to process, leading to denial of service. This issue only affects consumers using the strict option.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-32803

The npm package “tar” (aka node-tar) before versions 6.1.2, 5.0.7, 4.4.15, and 3.2.3 has an arbitrary File Creation/Overwrite vulnerability via insufficient symlink protection. `node-tar` aims to guarantee that any file whose location would be modified by a symbolic link is not extracted. This is, in part, achieved by ensuring that extracted directories are not symlinks. Additionally, in order to prevent unnecessary `stat` calls to determine whether a given path is a directory, paths are cached when directories are created. This logic was insufficient when extracting tar files that contained both a directory and a symlink with the same name as the directory. This order of operations resulted in the directory being created and added to the `node-tar` directory cache. When a directory is present in the directory cache, subsequent calls to mkdir for that directory are skipped. However, this is also where `node-tar` checks for symlinks occur. By first creating a directory, and then replacing that directory with a symlink, it was thus possible to bypass `node-tar` symlink checks on directories, essentially allowing an untrusted tar file to symlink into an arbitrary location and subsequently extracting arbitrary files into that location, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.3, 4.4.15, 5.0.7 and 6.1.2.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)

Vulnerability CVE-2021-32804

The npm package "tar" (aka node-tar) before versions 6.1.1, 5.0.6, 4.4.14, and 3.3.2 has a arbitrary File Creation/Overwrite vulnerability due to insufficient absolute path sanitization. node-tar aims to prevent extraction of absolute file paths by turning absolute paths into relative paths when the `preservePaths` flag is not set to `true`. This is achieved by stripping the absolute path root from any absolute file paths contained in a tar file. For example `/home/user/.bashrc` would turn into `home/user/.bashrc`. This logic was insufficient when file paths contained repeated path roots such as `////home/user/.bashrc`. `node-tar` would only strip a single path root from such paths. When given an absolute file path with repeating path roots, the resulting path (e.g. `///home/user/.bashrc`) would still resolve to an absolute path, thus allowing arbitrary file creation and overwrite. This issue was addressed in releases 3.2.2, 4.4.14, 5.0.6 and 6.1.1. Users may work around this vulnerability without upgrading by creating a custom `onentry` method which sanitizes the `entry.path` or a `filter` method which removes entries with absolute paths. See referenced GitHub Advisory for details. Be aware of CVE-2021-32803 which fixes a similar bug in later versions of tar.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-37701

The npm package "tar" (aka node-tar) before versions 4.4.16, 5.0.8, and 6.1.7 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability. node-tar aims to guarantee that any file whose location would be modified by a symbolic link is not extracted. This is, in part, achieved by ensuring that extracted directories are not symlinks. Additionally, in order to prevent unnecessary stat calls to determine whether a given path is a directory, paths are cached when directories are created. This logic was insufficient when extracting tar files that contained both a directory and a symlink with the same name as the directory, where the symlink and directory names in the archive entry used backslashes as a path separator on posix systems. The cache checking logic used both \ and / characters as path separators, however \ is a valid filename character on posix systems. By first creating a directory, and then replacing that directory with a symlink, it was thus possible to bypass node-tar symlink checks on directories, essentially allowing an untrusted tar file to symlink into an arbitrary location and subsequently extracting arbitrary files into that location, thus allowing arbitrary file creation and overwrite. Additionally, a similar confusion could arise on case-insensitive filesystems. If a tar archive contained a directory at `FOO`, followed by a symbolic link named `foo`, then on case-insensitive file systems, the creation of the symbolic link would remove the directory from the filesystem, but *not* from the internal directory cache, as it would not be treated as a cache hit. A subsequent file entry within the `FOO` directory would then be placed in the target of the symbolic link, thinking that the directory had already been created. These issues were addressed in releases 4.4.16, 5.0.8 and 6.1.7. The v3 branch of node-tar has been deprecated and did not receive patches for these issues. If you are still using a v3 release we recommend you update to a more recent version of node-tar. If this is not possible, a workaround is available in the referenced GHSA-9r2w-394v-53qc.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-59: Improper Link Resolution Before File Access ('Link Following')

Vulnerability CVE-2021-37712

The npm package “tar” (aka node-tar) before versions 4.4.18, 5.0.10, and 6.1.9 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability. node-tar aims to guarantee that any file whose location would be modified by a symbolic link is not extracted. This is, in part, achieved by ensuring that extracted directories are not symlinks. Additionally, in order to prevent unnecessary stat calls to determine whether a given path is a directory, paths are cached when directories are created. This logic was insufficient when extracting tar files that contained both a directory and a symlink with names containing unicode values that normalized to the same value. Additionally, on Windows systems, long path portions would resolve to the same file system entities as their 8.3 “short path” counterparts. A specially crafted tar archive could thus include a directory with one form of the path, followed by a symbolic link with a different string that resolves to the same file system entity, followed by a file using the first form. By first creating a directory, and then replacing that directory with a symlink that had a different apparent name that resolved to the same entry in the filesystem, it was thus possible to bypass node-tar symlink checks on directories, essentially allowing an untrusted tar file to symlink into an arbitrary location and subsequently extracting arbitrary files into that location, thus allowing arbitrary file creation and overwrite. These issues were addressed in releases 4.4.18, 5.0.10 and 6.1.9. The v3 branch of node-tar has been deprecated and did not receive patches for these issues. If you are still using a v3 release we recommend you update to a more recent version of node-tar. If this is not possible, a workaround is available in the referenced GHSA-qq89-hq3f-393p.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-59: Improper Link Resolution Before File Access (‘Link Following’)

Vulnerability CVE-2021-37713

The npm package “tar” (aka node-tar) before versions 4.4.18, 5.0.10, and 6.1.9 has an arbitrary file creation/overwrite and arbitrary code execution vulnerability. node-tar aims to guarantee that any file whose location would be outside of the extraction target directory is not extracted. This is, in part, accomplished by sanitizing absolute paths of entries within the archive, skipping archive entries that contain `..` path portions, and resolving the sanitized paths against the extraction target directory. This logic was insufficient on Windows systems when extracting tar files that contained a path that was not an absolute path, but specified a drive letter different from the extraction target, such as `C:some\path`. If the drive letter does not match the extraction target, for example `D:\extraction\dir`, then the result of `path.resolve(extractionDirectory, entryPath)` would resolve against the current working directory on the `C:` drive, rather than the extraction target directory. Additionally, a `..` portion of the path could occur immediately after the drive letter, such as `C:../foo`, and was not properly sanitized by the logic that checked for `..` within the normalized and split portions of the path. This only affects users of `node-tar` on Windows systems. These issues were addressed in releases 4.4.18, 5.0.10 and 6.1.9. The v3 branch of node-tar has been deprecated and did not receive patches for these issues. If you are still using a v3 release we recommend you update to a more recent version of node-tar. There is no reasonable way to work around this issue without performing the same path normalization procedures that node-tar now does. Users are encouraged to upgrade to the latest patched versions of node-tar, rather than attempt to sanitize paths themselves.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)

Vulnerability CVE-2021-39134

@npmcli/arborist, the library that calculates dependency trees and manages the node_modules folder hierarchy for the npm command line interface, aims to guarantee that package dependency contracts will be met, and the extraction of package contents will always be performed into the expected folder. This is, in part, accomplished by resolving dependency specifiers defined in package.json manifests for dependencies with a specific name, and nesting folders to resolve conflicting dependencies. When multiple dependencies differ only in the case of their name, Arborist's internal data structure saw them as separate items that could coexist within the same level in the node_modules hierarchy. However, on case-insensitive file systems (such as macOS and Windows), this is not the case. Combined with a symlink dependency such as file:/some/path, this allowed an attacker to create a situation in which arbitrary contents could be written to any location on the filesystem. For example, a package pwn-a could define a dependency in their package.json file such as "foo": "file:/some/path". Another package, pwn-b could define a dependency such as FOO: "file:foo.tgz". On case-insensitive file systems, if pwn-a was installed, and then pwn-b was installed afterwards, the contents of foo.tgz would be written to /some/path, and any existing contents of /some/path would be removed. Anyone using npm v7.20.6 or earlier on a case-insensitive filesystem is potentially affected. This is patched in @npmcli/arborist 2.8.2 which is included in npm v7.20.7 and above.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-61: UNIX Symbolic Link (Symlink) Following

Vulnerability CVE-2021-39135

@npmcli/arborist, the library that calculates dependency trees and manages the node_modules folder hierarchy for the npm command line interface, aims to guarantee that package dependency contracts will be met, and the extraction of package contents will always be performed into the expected folder. This is accomplished by extracting package contents into a project's node_modules folder. If the node_modules folder of the root project or any of its dependencies is somehow replaced with a symbolic link, it could allow Arborist to write package dependencies to any arbitrary location on the file system. Note that symbolic links contained within package artifact contents are filtered out, so another means of creating a node_modules symbolic link would have to be employed. 1. A preinstall script could replace node_modules with a symlink. (This is prevented by using --ignore-scripts.) 2. An attacker could supply the target with a git repository, instructing them to run npm install --ignore-scripts in the root. This may be successful, because npm install --ignore-scripts is typically not capable of making changes outside of the project directory, so it may be deemed safe. This is patched in @npmcli/arborist 2.8.2 which is included in npm v7.20.7 and above. For more information including workarounds please see the referenced GHSA-gmw6-94gg-2rc2.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-61: UNIX Symbolic Link (Symlink) Following

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-03-08): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.