SSA-943925: Multiple Vulnerabilities in SINEC NMS before V2.0 SP1

Publication Date: 2024-02-13
Last Update: 2024-03-12
Current Version: V1.1
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.4

SUMMARY

SINEC NMS before V2.0 SP1 is affected by multiple vulnerabilities.

Siemens has released an update for SINEC NMS and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC NMS: All versions < V2.0 SP1 affected by all CVEs	Update to V2.0 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109826954/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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 NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2022-4203

A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2022-4304

A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

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:U/RL:O/RC:C
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2022-4450

The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the “name” (e.g. “CERTIFICATE"), any header data and the payload data. If the function succeeds then the “name_out”, “header” and “data” arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.

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:U/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2023-0215

The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.

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:U/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2023-0216

An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack. The TLS implementation in OpenSSL does not call this function however third party applications might call these functions on untrusted data.

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-2023-0217

An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3.

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-2023-0286

There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

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:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-0401

A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data. In case the hash algorithm used for the signature is known to the OpenSSL library but the implementation of the hash algorithm is not available the digest initialization will fail. There is a missing check for the return value from the initialization function which later leads to invalid usage of the digest API most likely leading to a crash. The unavailability of an algorithm can be caused by using FIPS enabled configuration of providers or more commonly by not loading the legacy provider. PKCS7 data is processed by the SMIME library calls and also by the time stamp (TS) library calls. The TLS implementation in OpenSSL does not call these functions however third party applications would be affected if they call these functions to verify signatures on untrusted data.

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-2023-1255

Issue summary: The AES-XTS cipher decryption implementation for 64 bit ARM platform contains a bug that could cause it to read past the input buffer, leading to a crash.

Impact summary: Applications that use the AES-XTS algorithm on the 64 bit ARM platform can crash in rare circumstances. The AES-XTS algorithm is usually used for disk encryption.

The AES-XTS cipher decryption implementation for 64 bit ARM platform will read past the end of the ciphertext buffer if the ciphertext size is 4 mod 5 in 16 byte blocks, e.g. 144 bytes or 1024 bytes. If the memory after the ciphertext buffer is unmapped, this will trigger a crash which results in a denial of service.

If an attacker can control the size and location of the ciphertext buffer being decrypted by an application using AES-XTS on 64 bit ARM, the application is affected. This is fairly unlikely making this issue a Low severity one.

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-125: Out-of-bounds Read

Vulnerability CVE-2023-2454

schema_element defeats protective search_path changes; It was found that certain database calls in PostgreSQL could permit an authed attacker with elevated database-level privileges to execute arbitrary code.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-2455

Row security policies disregard user ID changes after inlining; PostgreSQL could permit incorrect policies to be applied in certain cases where role-specific policies are used and a given query is planned under one role and then executed under other roles. This scenario can happen under security definer functions or when a common user and query is planned initially and then re-used across multiple SET ROLEs. Applying an incorrect policy may permit a user to complete otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to define a row security policy.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-2650

Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(square(n)) with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low.

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:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2023-2975

Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be mislead by removing adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue.

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-287: Improper Authentication

Vulnerability CVE-2023-3446

Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

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-1333: Inefficient Regular Expression Complexity

Vulnerability CVE-2023-3817

Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

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-834: Excessive Iteration

Vulnerability CVE-2023-25690

Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

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-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Vulnerability CVE-2023-27522

HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

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-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Vulnerability CVE-2023-27533

A vulnerability in input validation exists in curl <8.0 during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and “telnet options” during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application’s intent. This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/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-2023-27534

A path traversal vulnerability exists in curl <8.0.0 SFTP implementation causes the tilde ( ) character to be wrongly replaced when used as a prefix in the first path element, in addition to its intended use as the first element to indicate a path relative to the user’s home directory. Attackers can exploit this flaw to bypass filtering or execute arbitrary code by crafting a path like / 2/foo while accessing a server with a specific user.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/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-2023-27535

An authentication bypass vulnerability exists in libcurl <8.0.0 in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2023-27536

An authentication bypass vulnerability exists libcurl <8.0.0 in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2023-27537

A double free vulnerability exists in libcurl <8.0.0 when sharing HSTS data between separate “handles”. This sharing was introduced without considerations for do this sharing across separate threads but there was no indication of this fact in the documentation. Due to missing mutexes or thread locks, two threads sharing the same HSTS data could end up doing a double-free or use-after-free.

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-415: Double Free

Vulnerability CVE-2023-27538

libcurl would reuse a previously created connection even when an SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, two SSH settings were left out from the configuration match checks, making them match too easily.

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-20: Improper Input Validation

Vulnerability CVE-2023-28319

A use after free vulnerability exists in curl <v8.1.0 in the way libcurl offers a feature to verify an SSH server’s public key using a SHA 256 hash. When this check fails, libcurl would free the memory for the fingerprint before it returns an error message containing the (now freed) hash. This flaw risks inserting sensitive heap-based data into the error message that might be shown to users or otherwise get leaked and revealed.

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-2023-28320

A denial of service vulnerability exists in curl <v8.1.0 in the way libcurl provides several different backends for resolving host names, selected at build time. If it is built to use the synchronous resolver, it allows name resolves to time-out slow operations using `alarm()` and `siglongjmp()`. When doing this, libcurl used a global buffer that was not mutex protected and a multi-threaded application might therefore crash or otherwise misbehave.

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-362: Concurrent Execution using Shared Resource with Improper Synchronization (’Race Condition’)

Vulnerability CVE-2023-28321

An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard patterns when listed as “Subject Alternative Name” in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one provided by a TLS library. This private wildcard matching function would match IDN (International Domain Name) hosts incorrectly and could as a result accept patterns that otherwise should mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always start with `xn--` and should not be allowed to pattern match, but the wildcard check in curl could still check for `x*`, which would match even though the IDN name most likely contained nothing even resembling an `x`.

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-295: Improper Certificate Validation

Vulnerability CVE-2023-28322

An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously wasused to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST.

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-28709

The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.

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-193: Off-by-one Error

Vulnerability CVE-2023-30581

The use of **proto** in process.mainModule.**proto**.require() can bypass the policy mechanism and require modules outside of the policy.json definition. This vulnerability affects all users using the experimental policy mechanism in all active release lines: v16, v18 and, v20.

Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-30582

A vulnerability in Node.js, affecting users of the experimental permission model when the –allow-fs-read flag is used with a non-* argument. This flaw arises from an inadequate permission model that fails to restrict file watching through the fs.watchFile API. As a result, malicious actors can monitor files that they do not have explicit read access to.

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-20: Improper Input Validation

Vulnerability CVE-2023-30583

fs.openAsBlob() can bypass the experimental permission model when using the file system read restriction with the –allow-fs-read flag in Node.js. This vulnerability arises from a missing check in the fs.openAsBlob() API.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-30584

A vulnerability in the experimental permission model of Node.js leads to improper handling of path traversal bypass when verifying file permissions.

CVSS v3.1 Base Score	7.7
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-30585

A vulnerability has been identified in the Node.js (.msi version) installation process, specifically affecting Windows users who install Node.js using the .msi installer. This vulnerability emerges during the repair operation, where the “msiexec.exe” process, running under the NT AUTHORITY\SYSTEM context, attempts to read the %USERPROFILE% environment variable from the current user’s registry.

The issue arises when the path referenced by the %USERPROFILE% environment variable does not exist. In such cases, the “msiexec.exe” process attempts to create the specified path in an unsafe manner, potentially leading to the creation of arbitrary folders in arbitrary locations.

The severity of this vulnerability is heightened by the fact that the %USERPROFILE% environment variable in the Windows registry can be modified by standard (or “non-privileged") users. Consequently, unprivileged actors, including malicious entities or trojans, can manipulate the environment variable key to deceive the privileged “msiexec.exe” process. This manipulation can result in the creation of folders in unintended and potentially malicious locations.

It is important to note that this vulnerability is specific to Windows users who install Node.js using the .msi installer. Users who opt for other installation methods are not affected by this particular issue.

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-30586

A privilege escalation vulnerability exists in Node.js 20 that allowed loading arbitrary OpenSSL engines when the experimental permission model is enabled, which can bypass and/or disable the permission model. The attack complexity is high. However, the crypto.setEngine() API can be used to bypass the permission model when called with a compatible OpenSSL engine. The OpenSSL engine can, for example, disable the permission model in the host process by manipulating the process’s stack memory to locate the permission model Permission::enabled_ in the host process’s heap memory. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

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-862: Missing Authorization

Vulnerability CVE-2023-30587

A vulnerability in Node.js allows for bypassing restrictions set by the –experimental-permission flag using the built-in inspector module (node:inspector). By exploiting the Worker class’s ability to create an “internal worker” with the kIsInternal Symbol, attackers can modify the isInternal value when an inspector is attached within the Worker constructor before initializing a new WorkerImpl.

CVSS v3.1 Base Score	6.2
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-30588

When an invalid public key is used to create an x509 certificate using the crypto.X509Certificate() API a non-expect termination occurs making it susceptible to DoS attacks when the attacker could force interruptions of application processing, as the process terminates when accessing public key info of provided certificates from user code. The current context of the users will be gone, and that will cause a DoS scenario. This vulnerability affects all active Node.js versions v16, v18, and, v20.

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-30589

The llhttp parser in the http module in Node v20.2.0 does not strictly use the CRLF sequence to delimit HTTP requests. This can lead to HTTP Request Smuggling (HRS).

The CR character (without LF) is sufficient to delimit HTTP header fields in the llhttp parser. According to RFC7230 section 3, only the CRLF sequence should delimit each header-field. This impacts all Node.js active versions: v16, v18, and, v20

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-30590

The generateKeys() API function returned from crypto.createDiffieHellman() only generates missing (or outdated) keys, that is, it only generates a private key if none has been set yet, but the function is also needed to compute the corresponding public key after calling setPrivateKey(). However, the documentation says this API call: “Generates private and public Diffie-Hellman key values”.

The documented behavior is very different from the actual behavior, and this difference could easily lead to security issues in applications that use these APIs as the DiffieHellman may be used as the basis for application-level security, implications are consequently broad.

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-31124

c-ares is an asynchronous resolver library. When cross-compiling c-ares and using the autotools build system, CARES_RANDOM_FILE will not be set, as seen when cross compiling aarch64 android. This will downgrade to using rand() as a fallback which could allow an attacker to take advantage of the lack of entropy by not using a CSPRNG. This issue was patched in version 1.19.1.

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-330: Use of Insufficiently Random Values

Vulnerability CVE-2023-31130

c-ares is an asynchronous resolver library. ares_inet_net_pton() is vulnerable to a buffer underflow for certain ipv6 addresses, in particular “0::00:00:00/2” was found to cause an issue. C-ares only uses this function internally for configuration purposes which would require an administrator to configure such an address via ares_set_sortlist(). However, users may externally use ares_inet_net_pton() for other purposes and thus be vulnerable to more severe issues. This issue has been fixed in 1.19.1.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-124: Buffer Underwrite (’Buffer Underflow’)

Vulnerability CVE-2023-31147

c-ares is an asynchronous resolver library. When /dev/urandom or RtlGenRandom() are unavailable, c-ares uses rand() to generate random numbers used for DNS query ids. This is not a CSPRNG, and it is also not seeded by srand() so will generate predictable output. Input from the random number generator is fed into a non-compilant RC4 implementation and may not be as strong as the original RC4 implementation. No attempt is made to look for modern OS-provided CSPRNGs like arc4random() that is widely available. This issue has been fixed in version 1.19.1.

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-330: Use of Insufficiently Random Values

Vulnerability CVE-2023-32002

The use of `Module._load()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module.

This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x.

Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.

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-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-32003

`fs.mkdtemp()` and `fs.mkdtempSync()` can be used to bypass the permission model check using a path traversal attack. This flaw arises from a missing check in the fs.mkdtemp() API and the impact is a malicious actor could create an arbitrary directory.

This vulnerability affects all users using the experimental permission model in Node.js 20.

Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

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-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2023-32004

A vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model. This flaw relates to improper handling of Buffers in file system APIs causing a traversal path to bypass when verifying file permissions.

This vulnerability affects all users using the experimental permission model in Node.js 20.

Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/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-2023-32005

A vulnerability has been identified in Node.js version 20, affecting users of the experimental permission model when the –allow-fs-read flag is used with a non-* argument.

This flaw arises from an inadequate permission model that fails to restrict file stats through the `fs.statfs` API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to.

This vulnerability affects all users using the experimental permission model in Node.js 20.

Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

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-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2023-32006

The use of `module.constructor.createRequire()` can bypass the policy mechanism and require modules outside of the policy.json definition for a given module.

This vulnerability affects all users using the experimental policy mechanism in all active release lines: 16.x, 18.x, and, 20.x.

Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-32067

c-ares is an asynchronous resolver library. c-ares is vulnerable to denial of service. If a target resolver sends a query, the attacker forges a malformed UDP packet with a length of 0 and returns them to the target resolver. The target resolver erroneously interprets the 0 length as a graceful shutdown of the connection. This issue has been patched in version 1.19.1.

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-2023-32558

The use of the deprecated API `process.binding()` can bypass the permission model through path traversal.

This vulnerability affects all users using the experimental permission model in Node.js 20.x.

Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

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-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2023-32559

A privilege escalation vulnerability exists in the experimental policy mechanism in all active release lines: 16.x, 18.x and, 20.x. The use of the deprecated API `process.binding()` can bypass the policy mechanism by requiring internal modules and eventually take advantage of `process.binding('spawn_sync')` run arbitrary code, outside of the limits defined in a `policy.json` file. Please note that at the time this CVE was issued, the policy is an experimental feature of Node.js.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-34035

Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.)

Specifically, an application is vulnerable when all of the following are true:

- Spring MVC is on the classpath
- Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet)
- The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints

An application is not vulnerable if any of the following is true:

- The application does not have Spring MVC on the classpath
- The application secures no servlets other than Spring MVC's DispatcherServlet
- The application uses requestMatchers(String) only for Spring MVC endpoints

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-863: Incorrect Authorization

Vulnerability CVE-2023-35945

Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's HTTP/2 codec may leak a header map and bookkeeping structures upon receiving `RST_STREAM` immediately followed by the `GOAWAY` frames from an upstream server. In nghttp2, cleanup of pending requests due to receipt of the `GOAWAY` frame skips de-allocation of the bookkeeping structure and pending compressed header. The error return [code path] is taken if connection is already marked for not sending more requests due to `GOAWAY` frame. The clean-up code is right after the return statement, causing memory leak. Denial of service through memory exhaustion. This vulnerability was patched in versions(s) 1.26.3, 1.25.8, 1.24.9, 1.23.11.

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-2023-38039

When curl retrieves an HTTP response, it stores the incoming headers so that they can be accessed later via the libcurl headers API.

However, curl did not have a limit in how many or how large headers it would accept in a response, allowing a malicious server to stream an endless series of headers and eventually cause curl to run out of heap 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-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2023-38199

coreruleset (aka OWASP ModSecurity Core Rule Set) through 3.3.4 does not detect multiple Content-Type request headers on some platforms. This might allow attackers to bypass a WAF with a crafted payload, aka “Content-Type confusion” between the WAF and the backend application. This occurs when the web application relies on only the last Content-Type header. Other platforms may reject the additional Content-Type header or merge conflicting headers, leading to detection as a malformed header.

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-843: Access of Resource Using Incompatible Type (’Type Confusion’)

Vulnerability CVE-2023-38545

This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake.

When curl is asked to pass along the hostname to the SOCKS5 proxy to allow that to resolve the address instead of it getting done by curl itself, the maximum length that hostname can be is 255 bytes.

If the hostname is detected to be longer than 255 bytes, curl switches to local name resolving and instead passes on the resolved address only to the proxy. Due to a bug, the local variable that means “let the host resolve the name” could get the wrong value during a slow SOCKS5 handshake, and contrary to the intention, copy the too long hostname to the target buffer instead of copying just the resolved address there.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2023-38546

This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met.

libcurl performs transfers. In its API, an application creates “easy handles” that are the individual handles for single transfers.

libcurl provides a function call that duplicates en easy handle called curl_easy_duphandle.

If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as `none` (using the four ASCII letters, no quotes).

Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named `none` - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.

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-73: External Control of File Name or Path

Vulnerability CVE-2023-39417

IN THE EXTENSION SCRIPT, a SQL Injection vulnerability was found in PostgreSQL if it uses @extowner@, @extschema@, or @extschema:...@ inside a quoting construct (dollar quoting, ‘’, or “”). If an administrator has installed files of a vulnerable, trusted, non-bundled extension, an attacker with database-level CREATE privilege can execute arbitrary code as the bootstrap superuser.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command (’SQL Injection’)

Vulnerability CVE-2023-39418

A vulnerability was found in PostgreSQL with the use of the MERGE command, which fails to test new rows against row security policies defined for UPDATE and SELECT. If UPDATE and SELECT policies forbid some rows that INSERT policies do not forbid, a user could store such rows.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2023-41080

URL Redirection to Untrusted Site (’Open Redirect’) vulnerability in FORM authentication feature Apache Tomcat.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M10, from 10.1.0-M1 through 10.0.12, from 9.0.0-M1 through 9.0.79 and from 8.5.0 through 8.5.92.

The vulnerability is limited to the ROOT (default) web application.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-601: URL Redirection to Untrusted Site (’Open Redirect’)

Vulnerability CVE-2023-46120

The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2024-23810

The affected application is vulnerable to SQL injection. This could allow an unauthenticated remote attacker to execute arbitrary SQL queries on the server database.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	9.4
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2024-23811

The affected application allows users to upload arbitrary files via TFTP. This could allow an attacker to upload malicious firmware images or other files, that could potentially lead to remote code execution.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	9.4
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2024-23812

The affected application incorrectly neutralizes special elements when creating a report which could lead to command injection.

CVSS v3.1 Base Score	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	9.4
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Thomas Riedmaier from Siemens Energy for reporting the vulnerability CVE-2024-23811

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 (2024-02-13): Publication Date
V1.1 (2024-03-12): Added missing acknowledgment for CVE-2024-23811

TERMS OF USE