TLP:WHITE

SICK PSIRT
Security Advisory

Vulnerability affecting picoScan and multiScan

Document ID:	SCA-2025-0006
Publication Date:	2025-04-28
CVE Identifiers:	CVE-2025-32472, CVE-2024-38517, CVE-2024-39684, CVE-2022-46908, CVE-2021-36690, CVE-2022-35737, CVE-2021-45346, CVE-2023-7104, CVE-2022-28805, CVE-2020-24370, CVE-2021-43519, CVE-2020-24369, CVE-2020-24371, CVE-2022-33099, CVE-2020-15945, CVE-2020-15888, CVE-2020-24342, CVE-2024-10525, CVE-2024-8376, CVE-2023-28366, CVE-2023-3592, CVE-2024-3935, CVE-2023-0809
Version:	2

Summary

SICK has identified a Denial of Service vulnerability (CVE-2025-32472) in picoScan and multiScan, which can cause the web page to become unresponsive. Due to their architectural design, these products are not affected by the other vulnerabilities listed in this advisory. Currently SICK is not aware of any public exploits specifically targeting the vulnerability. SICK recommends applying the mitigation for CVE-2025-32472.

List of Products

Product	Part Number	Affected by
SICK multiScan1XX all Firmware versions	1131164 1137723 1140110 1140133 1140134 1141496 1143873	CVE-2025-32472 Status: Known Affected Remediation: Workaround

		CVE-2024-38517 Status: Known Not Affected Remediation: -
		CVE-2024-39684 Status: Known Not Affected Remediation: -
		CVE-2022-46908 Status: Known Not Affected Remediation: -
		CVE-2021-36690 Status: Known Not Affected Remediation: -
		CVE-2022-35737 Status: Known Not Affected Remediation: -
		CVE-2021-45346 Status: Known Not Affected Remediation: -
		CVE-2023-7104 Status: Known Not Affected Remediation: -
		CVE-2022-28805 Status: Known Not Affected Remediation: -
		CVE-2020-24370 Status: Known Not Affected Remediation: -
		CVE-2021-43519 Status: Known Not Affected Remediation: -
		CVE-2020-24369 Status: Known Not Affected Remediation: -
		CVE-2020-24371 Status: Known Not Affected Remediation: -
		CVE-2022-33099 Status: Known Not Affected Remediation: -

		CVE-2020-15945 Status: Known Not Affected Remediation: -
		CVE-2020-15888 Status: Known Not Affected Remediation: -
		CVE-2020-24342 Status: Known Not Affected Remediation: -
		CVE-2024-10525 Status: Known Not Affected Remediation: -
		CVE-2024-8376 Status: Known Not Affected Remediation: -
		CVE-2023-28366 Status: Known Not Affected Remediation: -
		CVE-2023-3592 Status: Known Not Affected Remediation: -
		CVE-2024-3935 Status: Known Not Affected Remediation: -
		CVE-2023-0809 Status: Known Not Affected Remediation: -
SICK picoScan1XX all Firmware versions	1134607 1134608 1134609 1134610 1141395 1141396 1141397 1141751 1142269 1142270 1142272 1142273	CVE-2025-32472 Status: Known Affected Remediation: Workaround

		CVE-2024-38517 Status: Known Not Affected Remediation: -
		CVE-2024-39684 Status: Known Not Affected Remediation: -
		CVE-2022-46908 Status: Known Not Affected Remediation: -
		CVE-2021-36690 Status: Known Not Affected Remediation: -
		CVE-2022-35737 Status: Known Not Affected Remediation: -
		CVE-2021-45346 Status: Known Not Affected Remediation: -
		CVE-2023-7104 Status: Known Not Affected Remediation: -
		CVE-2022-28805 Status: Known Not Affected Remediation: -
		CVE-2020-24370 Status: Known Not Affected Remediation: -
		CVE-2021-43519 Status: Known Not Affected Remediation: -
		CVE-2020-24369 Status: Known Not Affected Remediation: -
		CVE-2020-24371 Status: Known Not Affected Remediation: -
		CVE-2022-33099 Status: Known Not Affected Remediation: -

		CVE-2020-15945 Status: Known Not Affected Remediation: -
		CVE-2020-15888 Status: Known Not Affected Remediation: -
		CVE-2020-24342 Status: Known Not Affected Remediation: -
		CVE-2024-10525 Status: Known Not Affected Remediation: -
		CVE-2024-8376 Status: Known Not Affected Remediation: -
		CVE-2023-28366 Status: Known Not Affected Remediation: -
		CVE-2023-3592 Status: Known Not Affected Remediation: -
		CVE-2024-3935 Status: Known Not Affected Remediation: -
		CVE-2023-0809 Status: Known Not Affected Remediation: -

Vulnerability Overview

CVE-2025-32472 Uncontrolled Resource Consumption

Summary: The multiScan and picoScan are vulnerable to a denial-of-service (DoS) attack. A remote attacker can exploit this vulnerability by conducting a Slowloris-type attack, causing the web page to become unresponsive.

CVE-2025-32472 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

CVE-2024-38517 Integer Underflow (Wrap or Wraparound)

Summary: Tencent RapidJSON is vulnerable to privilege escalation due to an integer underflow in the GenericReader::ParseNumber() function of include/rapidjson/reader.h when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer underflow vulnerability (when the file is parsed), leading to elevation of privilege.

CVE-2024-38517 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-191 (Integer Underflow (Wrap or Wraparound))

CVE-2024-39684 Integer Overflow or Wraparound

Summary: Tencent RapidJSON is vulnerable to privilege escalation due to an integer overflow in the GenericReader::ParseNumber() function of include/rapidjson/reader.h when parsing JSON text from a stream. An attacker needs to send the victim a crafted file which needs to be opened; this triggers the integer overflow vulnerability (when the file is parsed), leading to elevation of privilege.

CVE-2024-39684 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-190 (Integer Overflow or Wraparound)

CVE-2022-46908 Improper Access Control

Summary: SQLite through 3.40.0, when relying on --safe for execution of an untrusted CLI script, does not properly implement the azProhibitedFunctions protection mechanism, and instead allows UDF functions such as WRITEFILE.

CVE-2022-46908 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.3
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
CWE identifier: CWE-284 (Improper Access Control)

CVE-2021-36690 Improper Input Validation

Summary: A segmentation fault can occur in the sqlite3.exe command-line component of SQLite 3.36.0 via the idxGetTableInfo function when there is a crafted SQL query. NOTE: the vendor disputes the relevance of this report because a sqlite3.exe user already has full privileges (e.g., is intentionally allowed to execute commands). This report does NOT imply any problem in the SQLite library.

CVE-2021-36690 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-20 (Improper Input Validation)

CVE-2022-35737 Improper Validation of Array Index

Summary: SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.

CVE-2022-35737 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-129 (Improper Validation of Array Index)

CVE-2021-45346 Missing Release of Memory after Effective Lifetime

Summary: A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File), it is possible to query a record, and leak subsequent bytes of memory that extend beyond the record, which could let a malicious user obtain sensitive information. NOTE: The developer disputes this as a vulnerability stating that If you give SQLite a corrupted database file and submit a query against the database, it might read parts of the database that you did not intend or expect

CVE-2021-45346 has been assigned to this vulnerability.
CVSSv3.1 base score: 4.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-401 (Missing Release of Memory after Effective Lifetime)

CVE-2023-7104 Improper Restriction of Operations within the Bounds of a Memory Buffer

Summary: A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.

CVE-2023-7104 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
CWE identifier: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

CVE-2022-28805 Out-of-bounds Read

Summary: singlevar in lparser.c in Lua from (including) 5.4.0 up to (excluding) 5.4.4 lacks a certain luaK_exp2anyregup call, leading to a heap-based buffer over-read that might affect a system that compiles untrusted Lua code.

CVE-2022-28805 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
CWE identifier: CWE-125 (Out-of-bounds Read)

CVE-2020-24370 Integer Underflow (Wrap or Wraparound)

Summary: ldebug.c in Lua 5.4.0 allows a negation overflow and segmentation fault in getlocal and setlocal, as demonstrated by getlocal(3,2^31).

CVE-2020-24370 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE identifier: CWE-191 (Integer Underflow (Wrap or Wraparound))

CVE-2021-43519 Uncontrolled Recursion

Summary: Stack overflow in lua_resume of ldo.c in Lua Interpreter 5.1.0~5.4.4 allows attackers to perform a Denial of Service via a crafted script file.

CVE-2021-43519 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.5
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
CWE identifier: CWE-674 (Uncontrolled Recursion)

CVE-2020-24369 NULL Pointer Dereference

Summary: ldebug.c in Lua 5.4.0 attempts to access debug information via the line hook of a stripped function, leading to a NULL pointer dereference.

CVE-2020-24369 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-476 (NULL Pointer Dereference)

CVE-2020-24371 Release of Invalid Pointer or Reference

Summary: lgc.c in Lua 5.4.0 mishandles the interaction between barriers and the sweep phase, leading to a memory access violation involving collectgarbage.

CVE-2020-24371 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE identifier: CWE-763 (Release of Invalid Pointer or Reference)

CVE-2022-33099 Out-of-bounds Write

Summary: An issue in the component luaG_runerror of Lua v5.4.4 and below leads to a heap-buffer overflow when a recursive error occurs.

CVE-2022-33099 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-787 (Out-of-bounds Write)

CVE-2020-15945 Improper Handling of Values

Summary: Lua 5.4.0 (fixed in 5.4.1) has a segmentation fault in changedline in ldebug.c (e.g., when called by luaG_traceexec) because it incorrectly expects that an oldpc value is always updated upon a return of the flow of control to a function.

CVE-2020-15945 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.5
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-229 (Improper Handling of Values)

CVE-2020-15888 Heap-based Buffer Overflow

Summary: Lua through 5.4.0 mishandles the interaction between stack resizes and garbage collection, leading to a heap-based buffer overflow, heap-based buffer over-read, or use-after-free.

CVE-2020-15888 has been assigned to this vulnerability.
CVSSv3.1 base score: 8.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-122 (Heap-based Buffer Overflow)

CVE-2020-24342 Improper Restriction of Operations within the Bounds of a Memory Buffer

Summary: Lua through 5.4.0 allows a stack redzone cross in luaO_pushvfstring because a protection mechanism wrongly calls luaD_callnoyield twice in a row.

CVE-2020-24342 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

CVE-2024-10525 Out-of-bounds Write

Summary: In Eclipse Mosquitto, from version 1.3.2 through 2.0.18, if a malicious broker sends a crafted SUBACK packet with no reason codes, a client using libmosquitto may make out of bounds memory access when acting in its on_subscribe callback. This affects the mosquitto_sub and mosquitto_rr clients.

CVE-2024-10525 has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-787 (Out-of-bounds Write)

CVE-2024-8376 Missing Release of Memory after Effective Lifetime

Summary: In Eclipse Mosquitto up to version 2.0.18a, an attacker can achieve memory leaking, segmentation fault or heap-use-after-free by sending specific sequences of ”CONNECT”, ”DISCONNECT”, ”SUBSCRIBE”, ”UNSUBSCRIBE” and ”PUBLISH” packets.

CVE-2024-8376 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-401 (Missing Release of Memory after Effective Lifetime)

CVE-2023-28366 Missing Release of Memory after Effective Lifetime

Summary: The broker in Eclipse Mosquitto 1.3.2 through 2.x before 2.0.16 has a memory leak that can be abused remotely when a client sends many QoS 2 messages with duplicate message IDs, and fails to respond to PUBREC commands. This occurs because of mishandling of EAGAIN from the libc send function.

CVE-2023-28366 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-401 (Missing Release of Memory after Effective Lifetime)

CVE-2023-3592 Missing Release of Memory after Effective Lifetime

Summary: In Mosquitto before 2.0.16, a memory leak occurs when clients send v5 CONNECT packets with a will message that contains invalid property types.

CVE-2023-3592 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-401 (Missing Release of Memory after Effective Lifetime)

CVE-2024-3935 Double Free

Summary: In Eclipse Mosquito, versions from 2.0.0 through 2.0.18, if a Mosquitto broker is configured to create an outgoing bridge connection, and that bridge connection has an incoming topic configured that makes use of topic remapping, then if the remote connection sends a crafted PUBLISH packet to the broker a double free will occur with a subsequent crash of the broker.

CVE-2024-3935 has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-415 (Double Free)

CVE-2023-0809 Allocation of Resources Without Limits or Throttling

Summary: In Mosquitto before 2.0.16, excessive memory is allocated based on malicious initial packets that are not CONNECT packets.

CVE-2023-0809 has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

Remediations

Workaround for CVE-2025-32472

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices. Additionally, the web server can be disabled via the CyberSecurity page in the UI.

Valid for:

- SICK multiScan1XX all Firmware versions
- SICK picoScan1XX all Firmware versions

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.pdf

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2025-04-28	Initial version
2	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated