



Integer Truncation on SQLite

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-6965
State	PUBLISHED
Assigner	Google
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-15 14:15:31 UTC
Updated	2026-04-14 10:16:29 UTC
Description	There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from cve-coordination@google.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:N/AU:N/R:U/V:D/RE:L/U:Green

EPSS: 0.011820000 probability, percentile 0.787930000 (date 2026-04-15)

Problem Types: CWE-197 | CWE-197 CWE-197: Numeric Truncation Error

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@google.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality
Low

Integrity
High

Availability
Low

Sub Conf.
Low

Sub Integrity
High

Sub Availability
Low

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:N/AU:N/R:U/V:D/RE:L/U:Green

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sqlite	Sqlite	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	SQLite	SQLite	affected 3.50.2 semver	Not specified
ADP	Siemens	RUGGEDCOM CROSSBOW Station Access Controller SAC	affected V5.8 custom	Not specified
ADP	Siemens	SIDIS Prime	affected V4.0.800 custom	Not specified

References

Reference	Source	Link
seclists.org/fulldisclosure/2025/Sep/49	af854a3a-2127-422b-91ae-364da2661108	secli
seclists.org/fulldisclosure/2025/Sep/57	af854a3a-2127-422b-91ae-364da2661108	secli
www.sqlite.org/src/info/5508b56fd24016c13981ec280ecdd833007c9d8dd595edb295b9...	cve-coordination@google.com	www
www.openwall.com/lists/oss-security/2025/09/06/1	af854a3a-2127-422b-91ae-364da2661108	www
seclists.org/fulldisclosure/2025/Sep/53	af854a3a-2127-422b-91ae-364da2661108	secli
seclists.org/fulldisclosure/2025/Sep/56	af854a3a-2127-422b-91ae-364da2661108	secli
cert-portal.siemens.com/productcert/html/ssa-225816.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
cert-portal.siemens.com/productcert/html/ssa-485750.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
seclists.org/fulldisclosure/2025/Sep/58	af854a3a-2127-422b-91ae-364da2661108	secli
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

CNA: Vlad Stolyarov of Google's Threat Analysis Group, with assistance from Google Big Sleep (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)