Possible QML code injection in VectorImage component

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14576
State	PUBLISHED
Assigner	TQtC
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-30 13:16:02 UTC
Updated	2026-05-05 02:57:05 UTC
Description	Insufficient validation of node IDs in Qt SVG module allows arbitrary QML/JavaScript code injection when loading malicious

Risk And Classification

Primary CVSS: v4.0 7.4 HIGH from a59d8014-47c4-4630-ab43-e1b13cbe58e3

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

EPSS: 0.000090000 probability, percentile 0.008840000 (date 2026-05-05)

Problem Types: CWE-20 | CWE-94 | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection') | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	a59d8014-47c4-4630-ab43-e1b13cbe58e3	Secondary	7.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA
4.0	CNA	CVSS	7.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qt	Qtdeclarative	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	The Qt Company	Qt	affected 6.8.0 6.8.6 python	Windows, MacOS, Linux, iOS, Android, x86, ARM, 64 bit, 32 bit
CNA	The Qt Company	Qt	affected 6.10.0 6.10.1 python	Windows, MacOS, Linux, iOS, Android, x86, ARM, 64 bit, 32 bit

References

Reference	Source	Link	Tags
codereview.qt-project.org/c/qt/qtdeclarative/+/697273	a59d8014-47c4-4630-ab43-e1b13cbe58e3	codereview.qt-project.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: Qt Development Team (en)

Additional Advisory Data

Solutions

CNA: Update to Qt 6.8.7 or Qt 6.10.2 or later. As a temporary mitigation, validate and sanitize all SVG files before loading them with VectorImage, or only load SVG files from trusted sources.

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 registred 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**