



# XQUIC Improper STREAM Frame Validation in Initial/Handshake Packets

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

## Summary

<b>CVE</b>	CVE-2026-6328
<b>State</b>	PUBLISHED
<b>Assigner</b>	alibaba
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 04:17:48 UTC
<b>Updated</b>	2026-04-17 15:38:09 UTC
<b>Description</b>	Improper input validation, Improper verification of cryptographic signature vulnerability in XQUIC Project XQUIC xquic on Li

## Risk And Classification

**Primary CVSS:** v4.0 8.3 HIGH from alibaba-cna@list.alibaba-inc.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N/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:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000420000 probability, percentile 0.127410000 (date 2026-04-21)

**Problem Types:** CWE-20 | CWE-347 | CWE-20 CWE-20 Improper input validation | CWE-347 CWE-347 Improper verification of cryptographic signature

Version	Source	Type	Score	Severity	Vector
4.0	alibaba-cna@list.alibaba-inc.com	Secondary	8.3	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/S
4.0	CNA	CVSS	8.3	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/S

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

None  
 Confidentiality  
 Low  
 Integrity  
 High  
 Availability  
 None  
 Sub Conf.  
 None  
 Sub Integrity  
 None  
 Sub Availability  
 None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N/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:X/AU:X/R:X/V:X/RE:X/U:X

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">XQUIC Project</a>	XQUIC	affected 1.8.3 custom	Linux

#### References

Reference	Source	Link	Tag
github.com/alibaba/xquic/commit/4764604a0e487eeb49338b4498aecda2194eae84	alibaba-cna@list.alibaba-inc.com	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canc

No vendor comments have been submitted for this CVE.

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](#)