XQUIC Improper STREAM Frame Validation in Initial/Handshake Packets

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

Summary

CVE	CVE-2026-6328
State	PUBLISHED
Assigner	alibaba
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 04:17:48 UTC
Updated	2026-04-17 15:38:09 UTC
Description	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/MSC:X/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/MSC:X/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	XQUIC Project	XQUIC	affected 1.8.3 custom	Linux

References

Reference	Source	Link	Tags
github.com/alibaba/xquic/commit/4764604a0e487eeb49338b4498aecda2194eae84	alibaba-cna@list.alibaba-inc.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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