Elixir WebRTC: Missing DTLS peer fingerprint validation in ex_webrtc client-role handshake

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

Summary

CVE	CVE-2026-44700
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 21:16:47 UTC
Updated	2026-05-15 14:53:48 UTC
Description	Elixir WebRTC is an Elixir implementation of the W3C WebRTC API. Prior to 0.15.1 and 0.16.1, missing DTLS peer certifica

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/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: 0.000410000 probability, percentile 0.124130000 (date 2026-05-16)

Problem Types: CWE-295 | CWE-295 CWE-295: Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/S
4.0	CNA	DECLARED	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/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	Elixir-webrtc	Ex Webrtc	affected < 0.15.1	Not specified
CNA	Elixir-webrtc	Ex Webrtc	affected >= 0.16.0, < 0.16.1	Not specified

References

Reference	Source	Link	Tags
github.com/elixir-webrtc/ex_webrtc/pull/250	security-advisories@github.com	github.com	
github.com/elixir-webrtc/ex_webrtc/releases/tag/v0.16.1	security-advisories@github.com	github.com	
github.com/elixir-webrtc/ex_webrtc/security/advisories/GHSA-qwfw-ggxw-577c	security-advisories@github.com	github.com	
github.com/elixir-webrtc/ex_webrtc/issues/249	security-advisories@github.com	github.com	
github.com/elixir-webrtc/ex_webrtc/releases/tag/v0.15.1	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**