Insufficient Certificate Validation in Multiple Mobile Applications Allows Man in the Middle Interception

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-9293
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-13 02:16:46 UTC
Updated	2026-04-01 20:49:52 UTC
Description	A vulnerability in the certificate validation logic may allow applications to accept untrusted or improperly validated server ide

Risk And Classification

Primary CVSS: v4.0 7.7 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/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: 0.000130000 probability, percentile 0.019110000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:
4.0	CNA	CVSS	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/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	Tp-link	Aginet	All	All	All	All
Application	Tp-link	Deco	All	All	All	All
Application	Tp-link	Festa	All	All	All	All
Application	Tp-link	Kasa	All	All	All	All

Application	Tp-link	Kidshield	All	All	All	All
Application	Tp-link	Omada	All	All	All	All
Application	Tp-link	Omada Guard	All	All	All	All
Application	Tp-link	Tapo	All	All	All	All
Application	Tp-link	Tether	All	All	All	All
Application	Tp-link	Tp-partner	All	All	All	All
Application	Tp-link	Tpcamera	All	All	All	All
Application	Tp-link	Vigi	All	All	All	All
Application	Tp-link	Wi-fi Navi	All	All	All	All
Application	Tp-link	Wifi Toolkit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Tapo App	affected 3.14.111 custom	Android
CNA	TP-Link Systems Inc.	Kasa App	affected 3.4.350 custom	Android
CNA	TP Link Systems Inc.	Omada App	affected 4.25.25 custom	Android
CNA	TP-Link Systems Inc.	Omada Guard	affected 1.1.28 custom	Android
CNA	TP-Link Systems Inc.	Tether App	affected 4.12.27 custom	Android
CNA	TP-Link Systems Inc.	Deco App	affected 3.9.163 custom	Android
CNA	TP-Link Systems Inc.	Aginet App	affected 2.13.6 custom	Android
CNA	TP-Link Systems Inc.	TpCamera App	affected 3.2.17 custom	Android
CNA	TP-Link Systems Inc.	WiFi Toolkit	affected 1.4.28 custom	Android
CNA	TP-Link Systems Inc.	Festa App	affected 1.7.1 custom	Android
CNA	TP-Link Systems Inc.	Wi-Fi Navi	affected 1.5.5 custom	Android
CNA	TP-Link Systems Inc.	KidShield	affected 1.1.21 custom	Android
CNA	TP-Link Systems Inc.	TP-Partner App	affected 2.0.1 custom	Android
CNA	TP-Link Systems Inc.	VIGI App	affected 2.7.70 custom	Android

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/faq/4969	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
www.omadanetworks.com/us/support/faq/4969	f23511db-6c3e-4e32-a477-6aa17d310630	www.omadanetworks.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi

Vendor Comments And Credit

Discovery Credit

CNA: Francesco La Spina, Stanislav Dashevskyi from Forescout Technologies (en)

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