



CVE-2021-3275

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

Summary

CVE	CVE-2021-3275
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 13:15:00 UTC
Updated	2021-04-01 02:23:00 UTC
Description	Unauthenticated stored cross-site scripting (XSS) exists in multiple TP-Link products including WIFI Routers (Wireless AC r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer-c3150	-	All	All	All
Operating System	Tp-link	Archer-c3150 Firmware	v2_170926	All	All	All
Hardware	Tp-link	Td-w9977	-	All	All	All
Operating System	Tp-link	Td-w9977 Firmware	v1_0.1.0_0.9.1_up_boot\{161123\}_2016-11-23_15.36.15	All	All	All
Hardware	Tp-link	Tl-wa801n	-	All	All	All
Hardware	Tp-link	Tl-wa801nd	-	All	All	All
Operating System	Tp-link	Tl-wa801nd Firmware	v5_us_0.9.1_3.16_up_boot\{170905-rel56404\}	All	All	All
Operating System	Tp-link	Tl-wa801n Firmware	v6_eu_0.9.1_3.16_up_boot\{200116-rel61815\}	All	All	All
Hardware	Tp-link	Tl-wr802n	-	All	All	All
Operating System	Tp-link	Tl-wr802n Firmware	v4_us_0.9.1_3.17_up_boot\{200421-rel38950\}	All	All	All

References

Reference	Source	Link
TP-Link Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com
Full Disclosure: CVE-2021-3275 : Unauthenticated Stored Cross-site Scripting in Multiple TP-Link Devices	FULLDISC	seclists.org
WiFi Networking Equipment for Home & Business TP-Link	MISC	www.tp-link.com
CVE/CVE-2021-3275 at main · smriti548/CVE · GitHub	MISC	github.com

