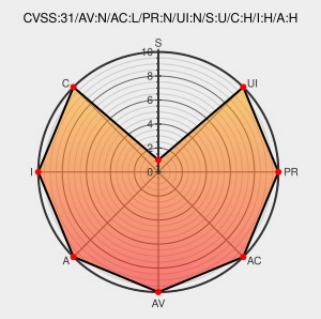
CVE-2022-37860

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-37860

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of M7350 from Tp-link contain the following vulnerability:

The web configuration interface of the TP-Link M7350 V3 with firmware version 190531 is affected by a pre-authentication command injection vulnerability.

CVE-2022-37860 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Download for M7350 | TP-Link United Kingdom	www.tp-link.com text/html	MISC www.tp-link.com/uk/support/download/m7350/v3/#Firmware
语雀	www.yuque.com text/html	MISC www.yuque.com/docs/share/fca60ef9-e5a4-462a-a984-61def4c9b132

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	M7350	v3	All	All	All
Operating System	Tp-link	M7350 Firmware	190531	All	All	All
Hardware	Tp-link	M7350 V3	All	All	All	All

cpe:2.3:h:tp-link:m7350:v3:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:m7350_firmware:190531:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:m7350_v3:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-37860 The web configuration interface of the TP-Link M7350 V3 with firm… twitter.com/i/web/status/1…	2022-09-12 17:55:55
@CVEreport	CVE-2022-37860 : The web configuration interface of the TP-Link M7350 V3 with firmware version 190531 is affected b… twitter.com/i/web/status/1…	2022-09-12 18:02:50
@Inceptus3	New Vulnerability: CVE-2022-37860 #InceptusSecure #UnderOurProtection	2022-09-12 20:13:17
/r/netcve	CVE-2022-37860	2022-09-12 18:38:40

← Previous ID

Next ID→