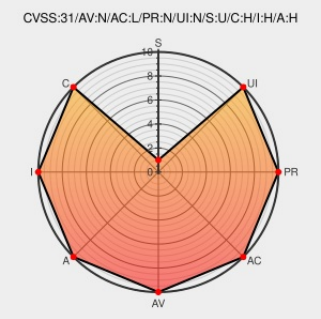
CVE-2021-31573

Published on: Not Yet Published

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

CVE-2021-31573

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



Certain versions of En7528 from Mediatek contain the following vulnerability:

In Config Manager, there is a possible command injection due to improper input validation. This could lead to remote escalation of privilege from a proximal attacker with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: A20210009; Issue ID: OSBNB00123234.

CVE-2021-31573 has been assigned by security@mediatek.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **MediaTek, Inc.** - **EN7528, EN7580** version **Linux SDK versions less than TLM7.3.275.0-82**

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
Product Security Acknowledgements	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-acknowledgements

There are currently no QIDs associated with this CVE

Exploit/POC from Github

In Config Manager, there is a possible command injection due to improper input validation. This could lead to remote …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mediatek	En7528	-	All	All	All
Operating System	Mediatek	En7528 Firmware	All	All	All	All
Hardware	Mediatek	En7580	-	All	All	All
Operating System	Mediatek	En7580 Firmware	All	All	All	All

cpe:2.3:h:mediatek:en7528:-:*:*:*:*:*:*:*:

cpe:2.3:o:mediatek:en7528_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:en7580:-:*:*:*:*:*:*:*:

cpe:2.3:o:mediatek:en7580_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31573 : In Config Manager, there is a possible command injection due to improper input validation. This co… twitter.com/i/web/status/1…	2023-02-06 22:07:50
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-31573 In Config Manager, there is a possible command injection due to i… twitter.com/i/web/status/1…	2023-02-06 22:55:56
@JohnJasonFallow	New vulnerability on the NVD: CVE-2021-31573 ift.tt/oGar1EM	2023-02-06 23:17:27
@doogsineerg	New vulnerability on the NVD: CVE-2021-31573 ift.tt/IaKt6H8	2023-02-06 23:33:48
@xanadulinux	CVE-2021-31573 ift.tt/kXzupEm	2023-02-06 23:53:26
/r/netcve	CVE-2021-31573	2023-02-06 23:38:30

← Previous ID

Next ID→

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