



CVE-2021-31577

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-31577

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [En7528](#) from [Mediatek](#) contain the following vulnerability:

In Boa, there is a possible escalation of privilege due to a missing permission check. 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: A20210008; Issue ID: OSBNB00123241.

CVE-2021-31577 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 TLM7.3.275.0-64**

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

Exploit/POC from Github

In Boa, there is a possible escalation of privilege due to a missing permission check. This could lead to remote esca...

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-2021-31577 : In Boa, there is a possible escalation of privilege due to a missing permission check. This could... twitter.com/i/web/status/1...	2023-02-06 22:09:26
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2021-31577 ift.tt/AuOHakY	2023-02-06 23:17:24
 @doogsineerg	New vulnerability on the NVD: CVE-2021-31577 ift.tt/IsDSUHx	2023-02-06 23:33:45
 @xanadulinux	CVE-2021-31577 ift.tt/wkLiGs0	2023-02-06 23:53:24
 @threatmeter	CVE-2021-31577 MediaTek CPU Boa permission A vulnerability was found in MediaTek CPU. It has been rated as critic... twitter.com/i/web/status/1...	2023-02-07 08:51:02
 /r/netcve	CVE-2021-31577	2023-02-06 23:38:33

[← Previous ID](#)

[Next ID →](#)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)