



CVE-2022-24011

Published on: Not Yet Published

Last Modified on: 08/09/2022 07:28:00 PM UTC

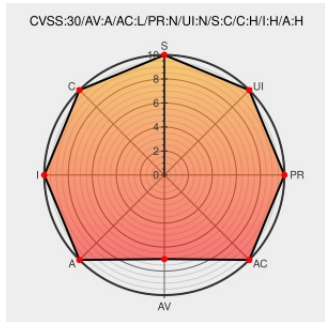
CVE-2022-24011

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linkhub Mesh Wifi Ac1200](#) from [Tcl](#) contain the following vulnerability:

A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability. This vulnerability represents all occurrences of the buffer overflow vulnerability within the device_list binary.

CVE-2022-24011 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [TCL](#) - [LinkHub Mesh Wifi](#) version = [MS1G_00_01.00_14](#)

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
TALOS-2022-1463 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1463

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Tcl	Linkhub Mesh Wifi Ac1200	-	All	All	All
Operating System	Tcl	Linkhub Mesh Wifi Ac1200	ms1g_00_01.00_14	All	All	All

```
cpe:2.3:h:tcl:linkhub_mesh_wifi_ac1200:-:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:tcl:linkhub_mesh_wifi_ac1200:ms1g_00_01.00_14:*:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-24011 : A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1... twitter.com/i/web/status/1...	2022-08-05 21:37:05
 @threatmeter	CVE-2022-24011 A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_... twitter.com/i/web/status/1...	2022-08-06 07:10:01
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-24011 - A buffer overflow vulnerability exists in the GetValue functionality... twitter.com/i/web/status/1...	2022-08-09 19:42:14
 /r/netcve	CVE-2022-24011	2022-08-05 22:38:47

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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