



CVE-2019-7163

Published on: 08/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:53 PM UTC

CVE-2019-7163

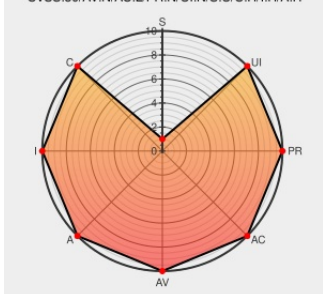
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Alcatel Linkzone](#) from [Tcl](#) contain the following vulnerability:

The web interface of Alcatel LINKZONE MW40-V-V1.0 MW40_LU_02.00_02 devices is vulnerable to an authentication bypass that allows an unauthenticated user to have access to the web interface without knowing the administrator's password.

CVE-2019-7163 has been assigned by [M](#) 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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
D-Link DVA-5592 missing authentication check [CVE-2019-6969] D-Link DVA-5592 Self XSS [CVE-2019-6968] Alcatel LINKZONE no authentication control whatsoever [CVE-2019-7163]	Exploit Third Party Advisory rhaidiz.net text/html	MISC rhaidiz.net/2019/02/27/dribble-router-vulns-dlink-alcatel-cve-2019-6969-cve-2019-6968-cve-2019-7163/">rhaidiz.net/2019/02/27/dribble-router-vulns-dlink-alcatel-cve-2019-6969-cve-2019-6968-cve-2019-7163/

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	Alcatel Linkzone	-	All	All	All
Hardware 	Tcl	Alcatel Linkzone	-	All	All	All
Operating System	Tcl	Alcatel Linkzone Firmware	mw40-v-v1.0_mw40_lu_02.00_02	All	All	All
Operating System	Tcl	Alcatel Linkzone Firmware	mw40-v-v1.0_mw40_lu_02.00_02	All	All	All
cpe:2.3:h:tcl:alcatel_linkzone:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:tcl:alcatel_linkzone:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:tcl:alcatel_linkzone_firmware:mw40-v-v1.0_mw40_lu_02.00_02:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:tcl:alcatel_linkzone_firmware:mw40-v-v1.0_mw40_lu_02.00_02:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)