



CVE-2022-47699

Published on: Not Yet Published

Last Modified on: 02/08/2023 03:15:00 PM UTC

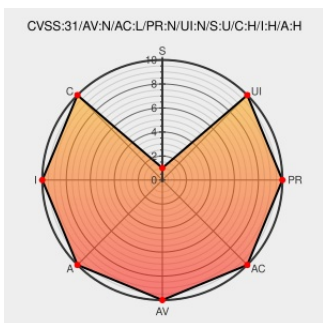
CVE-2022-47699

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Cf-wr623n](#) from [Comfast Project](#) contain the following vulnerability:

COMFAST (Shenzhen Sihai Zhonglian Network Technology Co., Ltd) CF-WR623N Router firmware V2.3.0.1 is vulnerable to Incorrect Access Control.

CVE-2022-47699 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

CVE References

Description

Tags

Link

cve/password_pol_bypass.md at main · OlivierLaflamme/cve · GitHub

[github.com](#)
[text/html](#)

MISC
github.com/OlivierLaflamme/cve/blob/main/COMFAST/CF-WR623N/password_pol_bypass.md

Page not found · GitHub · GitHub

[github.com](#)
[text/html](#)
Inactive Link **Not Archived**

MISC
github.com/OlivierLaflamme/cve/blob/main/COMFAST/CF-WR623N/password_pol_bypass

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

COMFAST (Shenzhen Sihai Zhonglian Network Technology Co., Ltd) CF-WR623N Router firmware V2.3.0.1 is vulnerable to In...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Comfast Project	Cf-wr623n	-	All	All	All
Operating System	Comfast Project	Cf-wr623n Firmware	2.3.0.1	All	All	All
cpe:2.3:h:comfast_project:cf-wr623n:-:*:*:*:*:*:						
cpe:2.3:o:comfast_project:cf-wr623n_firmware:2.3.0.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-47699 : COMFAST Shenzhen Sihai Zhonglian Network Technology Co., Ltd CF-WR623N Router firmware V2.3.0.1... twitter.com/i/web/status/1...	2023-01-31 18:03:56
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-47699 COMFAST (Shenzhen Sihai Zhonglian Network Technology Co., Ltd) CF... twitter.com/i/web/status/1...	2023-01-31 18:56:00
 /r/netcve	CVE-2022-47699	2023-01-31 19:39:08

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)