

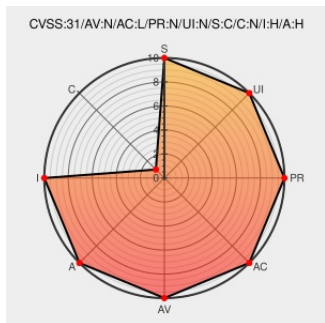


CVE-2020-8974

Published on: Not Yet Published

Last Modified on: 10/21/2022 08:22:00 PM UTC

CVE-2020-8974 - advisory for INCIBE-2022-0936

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of **Zgr Tps200 Ng** from **Zigor** contain the following vulnerability:

In ZGR TPS200 NG 2.00 firmware version and 1.01 hardware version, the firmware upload process does not perform any type of restriction. This allows an attacker to modify it and re-upload it via web with malicious modifications, rendering the device unusable.

CVE-2020-8974 has been assigned by [cve-coordination@incibe.es](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **ZGR - ZGR TPS200 NG** version = **firmware version 2.00**

Affected Vendor/Software: **ZGR - ZGR TPS200 NG** version = **hardware version 1.01**

CVSS3 Score: **9.1 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	HIGH

CVE References

Description	Tags	Link
Multiple vulnerabilities in ZGR TPS200 NG INCIBE-CERT	www.incibe-cert.es text/html	CONFIRM www.incibe-cert.es/en/early-warning/ics-advisories/multiple-vulnerabilities-zgr-tps200-ng

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 	Zigor	Zgr Tps200 Ng	1.01	All	All	All
Operating System	Zigor	Zgr Tps200 Ng Firmware	2.00	All	All	All
cpe:2.3:h:zigor:zgr_tps200_ng:1.01:*****:						
cpe:2.3:o:zigor:zgr_tps200_ng_firmware:2.00:*****:						

Discovery Credit

Discovered by the Industrial Cybersecurity team of S21sec, special mention to Aaron Flecha Menéndez.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-8974 : In ZGR TPS200 NG 2.00 firmware version and 1.01 hardware version, the firmware upload process does... twitter.com/i/web/status/1...	2022-10-17 22:06:34
 /r/netcve	CVE-2020-8974	2022-10-17 23:38:09

[← 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](#)