



CVE-2021-41290

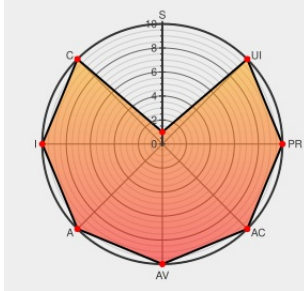
Published on: 09/30/2021 12:00:00 AM UTC

Last Modified on: 10/21/2022 05:46:00 PM UTC

CVE-2021-41290 - advisory for TVN-202109006

[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 [Ecs Router Controller-ecs](#) from [Ecoa](#) contain the following vulnerability:

ECOAS controller suffers from an arbitrary file write and path traversal vulnerability. Using the POST parameters, unauthenticated attackers can remotely set arbitrary values for location and content type and gain the possibility to execute arbitrary code on the affected device.

CVE-2021-41290 has been assigned by [cve@cert.org.tw](#) 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: **10 - HIGH**

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

CVE References

Description	Tags	Link
TWCERT/CC台灣電腦網路危機處理暨協調中心-ECOAS controller - Path Traversal-1	www.twcert.org.tw text/html	MISC www.twcert.org.tw/tw/cp-132-5126-ca315-1.html

By selecting these links, you may be leaving CVEreport webpages. We have provided these links to other websites because they may have information that

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

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-41290 : ECOA BAS controller suffers from an arbitrary file write and path traversal vulnerability. Using t... twitter.com/i/web/status/1...	2021-09-30 10:47:41

[← Previous ID](#)

Next ID→

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](#)