



CVE-2021-41292

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

Last Modified on: 04/25/2022 05:59:00 PM UTC

CVE-2021-41292 - advisory for TVN-202109008

[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 authentication bypass vulnerability. An unauthenticated attacker through cookie poisoning can remotely bypass authentication and disclose sensitive information and circumvent physical access controls in smart homes and buildings and manipulate HVAC.

CVE-2021-41292 has been assigned by [cve@cert.org.tw](#) to track the vulnerability - currently rated as **CRITICAL** severity.

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	HIGH	HIGH	NONE

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
TWCERT/CC-台灣電腦網路危機處理暨協調中心-ECOAS controller - Broken Authentication	www.twcert.org.tw text/html	MISC www.twcert.org.tw/tw/cp-132-5128-b075a-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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Ecoa	Ecs Router Controller-ecs	-	All	All	All
Operating System	Ecoa	Ecs Router Controller-ecs Firmware	-	All	All	All
Hardware 	Ecoa	Riskbuster	-	All	All	All
Operating System	Ecoa	Riskbuster Firmware	-	All	All	All
Application	Ecoa	Riskterminator	-	All	All	All
cpe:2.3:h:ecoa:ecs_router_controller-ecs:-:*:*:*:*:*:						
cpe:2.3:o:ecoa:ecs_router_controller-ecs_firmware:-:*:*:*:*:*:						
cpe:2.3:h:ecoa:riskbuster:-:*:*:*:*:*:						
cpe:2.3:o:ecoa:riskbuster_firmware:-:*:*:*:*:*:						
cpe:2.3:a:ecoa:riskterminator:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-41292 : ECOA BAS controller suffers from an authentication bypass vulnerability. An unauthenticated attack... twitter.com/i/web/status/1...	2021-09-30 10:48:34
 @threatmeter	CVE-2021-41292 ECOA BAS controller suffers from an authentication bypass vulnerability. An unauthenticated attacker... twitter.com/i/web/status/1...	2021-10-01 07:09:48

[← 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](#).

