

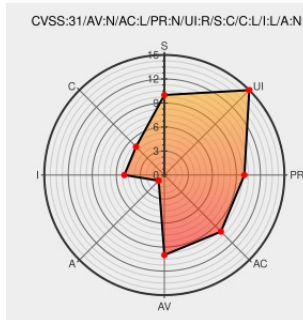


CVE-2021-43106

Published on: Not Yet Published

Last Modified on: 02/23/2022 02:01:00 AM UTC

CVE-2021-43106

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

Certain versions of [Tranzware Online](#) from [Compassplus](#) contain the following vulnerability:

A Header Injection vulnerability exists in Compass Plus TranzWare Online FIMI Web Interface Tranzware Online (TWO) 5.3.33.3 F38 and FIMI 4.2.19.4 25. The HTTP host header can be manipulated and cause the application to behave in unexpected ways. Any changes made to the header would just cause the request to be sent to a

completely different Domain/IP address. This is due to that the server implicitly trusts the Host header, and fails to validate or escape it properly. An attacker can use this input to redirect target users to a malicious domain/web page. This would result in expanding the potential to further attacks and malicious actions.

CVE-2021-43106 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description

CompassPlus/TranzWare Online FIMI_Version 4.2.19.4 25_HHI at main · lthacaLabs/CompassPlus · GitHub

Tags

github.com

text/html

Link

MISC
github.com/lthacaLabs/CompassPlus/tree/main/TranzWare%20Online%20FIMI_Version%204.2.19.4

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
Application	Compassplus	Tranzware Online	5.3.33.3_f38	All	All	All
Application	Compassplus	Tranzware Online Financial Institution Maintenance Interface	4.2.19.4.25	All	All	All

cpe:2.3:a:compassplus:tranzware_online:5.3.33.3_f38:*:*:*:*:*:

cpe:2.3:a:compassplus:tranzware_online_financial_institution_maintenance_interface:4.2.19.4.25:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43106 : A Header Injection vulnerability exists in Compass Plus TranzWare Online FIMI Web Interface Tranzw... twitter.com/i/web/status/1...	2022-02-14 20:08:53
/r/netcve	CVE-2021-43106	2022-02-14 21:38:50

← 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](#)