



CVE-2021-40845

Published on: 09/15/2021 12:00:00 AM UTC

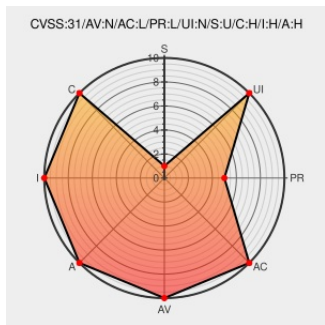
Last Modified on: 09/27/2021 08:52:00 PM UTC

CVE-2021-40845

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Alphacom Xe Audio Server](#) from [Zenitel](#) contain the following vulnerability:

The web part of Zenitel AlphaCom XE Audio Server through 11.2.3.10, called AlphaWeb XE, does not restrict file upload in the Custom Scripts section at `php/index.php`. Neither the content nor extension of the uploaded files is checked, allowing execution of PHP code under the `/cmd` directory.

CVE-2021-40845 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Zenitel AlphaCom XE Audio Server 11.2.3.10 Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/164160/Zenitel-AlphaCom-XE-Audio-Server-11.2.3.10-Shell-Upload.html

GitHub - ricardojoserf/CVE-2021-40845: AlphaWeb XE, the embedded web server running on AlphaCom XE, has a vulnerability which allows to upload PHP files leading to RCE once the authentication is successful.

github.com
text/html

MISC github.com/ricardojoserf/CVE-2021-40845

CVE-2021-40845 - AlphaWeb Authenticated RCE – Ricardo Ruiz – Pentesting, scripting and dumb ideas!

ricardojoserf.github.io
text/html

MISC ricardojoserf.github.io/CVE-2021-40845/

Zenitel AlphaCom XE Audio Server 11.2.3.10 Shell Upload ≈ Packet Storm

packetstormsecurity.com
text/html

MISC packetstormsecurity.com/files/164149/Zenitel-AlphaCom-XE-Audio-Server-11.2.3.10-Shell-Upload.html

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	Zenitel	Alphacom Xe Audio Server	All	All	All	All
cpe:2.3:a:zenitel:alphacom_xe_audio_server:*.***.***.***:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-40845 : The web part of Zenitel AlphaCom XE Audio Server through 11.2.3.10, called AlphaWeb XE, does not r... twitter.com/i/web/status/1...	2021-09-15 13:06:15
@SecurityNewsbot	Zenitel AlphaCom XE Audio Server 11.2.3.10 Shell Upload packetstormsecurity.com/files/164160/C... #PacketStorm	2021-09-17 07:30:08

← Previous ID

Next ID →

© CVE.report 2021 |

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report