



CVE-2021-41554

Published on: 10/05/2021 12:00:00 AM UTC

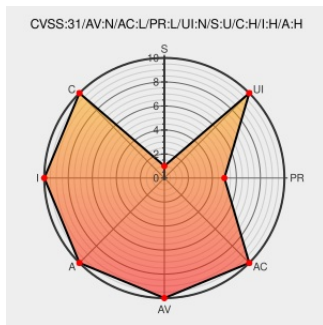
Last Modified on: 10/09/2021 03:28:00 AM UTC

CVE-2021-41554

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Web Central](#) from [Archibus](#) contain the following vulnerability:

**** UNSUPPORTED WHEN ASSIGNED **** ARCHIBUS Web Central 21.3.3.815 (a version from 2014) does not properly validate requests for access to data and functionality in these affected endpoints: /archibus/schema/ab-edit-users.axvw, /archibus/schema/ab-data-dictionary-table.axvw, /archibus/schema/ab-schema-add-field.axvw,

/archibus/schema/ab-core/views/process-navigator/ab-my-user-profile.axvw. By not verifying the permissions for access to resources, it allows a potential attacker to view pages that are not allowed. Specifically, it was found that any authenticated user can reach the administrative console for user management by directly requesting access to the page via URL. This allows a malicious user to modify all users' profiles, to elevate any privileges to administrative ones, or to create or delete any type of user. It is also possible to modify the emails of other users, through a misconfiguration of the username parameter, on the user profile page. This is fixed in all recent versions, such as version 26. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Version 21.3 was officially de-supported by the end of 2020.

CVE-2021-41554 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
Gruppo TIM Vulnerability Research & Advisor	www.gruppotim.it text/html	 MISC www.gruppotim.it/redteam

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	Archibus	Web Central	21.3.3.815	All	All	All
<code>cpe:2.3:a:archibus:web_central:21.3.3.815:****:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-41554 : ARCHIBUS Web Central 21.3.3.815 a version from 2014 does not properly validate requests for ac... twitter.com/i/web/status/1...	2021-10-05 15:05:32
 @RedPacketSec	CVE-2021-41554 - redpacketsecurity.com/cve-2021-41554/ #cybersecurity	2021-10-09 14:51:15