

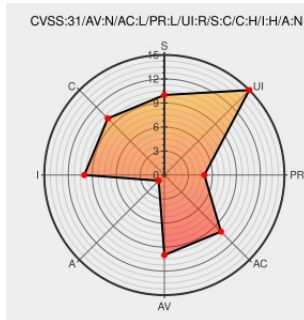


CVE-2021-43853

Published on: Not Yet Published

Last Modified on: 08/09/2022 01:28:00 PM UTC

CVE-2021-43853 - advisory for GHSA-5q7q-qqw2-hjq7

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

Certain versions of [Ajax.net Professional](#) from [Ajax.net Professional Project](#) contain the following vulnerability:

Ajax.NET Professional (AjaxPro) is an AJAX framework available for Microsoft ASP.NET. Affected versions of this package are vulnerable to JavaScript object injection which may result in cross site scripting when leveraged by a malicious user. The affected core relates to JavaScript object creation when parsing json input. Releases before version

21.12.22.1 are affected. A workaround exists that replaces one of the core JavaScript files embedded in the library. See the GHSA-5q7q-qqw2-hjq7 for workaround details.

CVE-2021-43853 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [michaelschwarz](#) - [Ajax.NET-Professional](#) version < 21.12.22.1

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

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

CVE References

Description	Tags	Link				
Release v21.12.22.1 · michaelsschwarz/Ajax.NET-Professional · GitHub	github.com text/html	 MISC github.com/michaelsschwarz/Ajax.NET-Professional/releases/tag/v21.12.22.1				
fixed another XSS issue · michaelsschwarz/Ajax.NET-Professional@c89e39b · GitHub	github.com text/html	 MISC github.com/michaelsschwarz/Ajax.NET-Professional/commit/c89e39b9679fcb8ab6644fe21cc7e652cb615e2b				
Cross-Site Scripting Security Vulnerability · Advisory · michaelsschwarz/Ajax.NET-Professional · GitHub	github.com text/html	 CONFIRM github.com/michaelsschwarz/Ajax.NET-Professional/security/advisories/GHSA-5q7q-qqw2-hjq7				
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	Ajax.net Professional Project	Ajax.net Professional	All	All	All	All
cpe:2.3:a:ajax.net_professional_project:ajax.net_professional:*.~.						