



CVE-2021-34821

Published on: 07/19/2021 12:00:00 AM UTC

Last Modified on: 07/28/2021 05:02:00 PM UTC

CVE-2021-34821

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Novus Management System](#) from [Aat](#) contain the following vulnerability:

Cross Site Scripting (XSS) vulnerability exists in AAT Novus Management System through 1.51.2. The WebUI has wrong HTTP 404 error handling implemented. A remote, unauthenticated attacker may be able to exploit the issue by sending malicious HTTP requests to non-existing URLs. The value of the URL path filename is copied into the HTML document as plain text tags.

CVE-2021-34821 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: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Full Disclosure: Novus Managment System Vulnerabilities (CVE-2021-34820, CVE-2021-38421)	seclists.org text/html	FULLDISC FULLDISC: 20210709 Novus Managment System Vulnerabilities (CVE-2021-34820, CVE-2021-38421)

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	Aat	Novus Management System	All	All	All	All
cpe:2.3:a:aat:novus_management_system:*****:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-34821 : Cross Site Scripting #XSS vulnerability exists in AAT Novus Management System through 1.51.2. Th... twitter.com/i/web/status/1...	2021-07-19 18:07:38
 @SecRiskRptSME	RT: CVE-2021-34821 Cross Site Scripting (XSS) vulnerability exists in AAT Novus Management System through 1.51.2.... twitter.com/i/web/status/1...	2021-07-20 07:21:22
 /r/netcve	CVE-2021-34821	2021-07-19 18:40:28

[← 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](#)