



CVE-2021-25976

Published on: 11/16/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 06:44:00 PM UTC

CVE-2021-25976 - advisory for <https://www.whitesourcesoftware.com/vulnerability-database/>

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H



Certain versions of [Piranha Cms](#) from [Dotnetfoundation](#) contain the following vulnerability:

In PiranhaCMS, versions 4.0.0-alpha1 to 9.2.0 are vulnerable to cross-site request forgery (CSRF) when performing various actions supported by the management system, such as deleting a user, deleting a role, editing a post, deleting a media folder etc., when an ID is known.

CVE-2021-25976 has been assigned by [vulnerabilitylab@whitesourcesoftware.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [PiranhaCMS](#) - Piranha version $\geq$ 4.0.0-alpha1

Affected Vendor/Software: [PiranhaCMS](#) - Piranha version $\leq$ 9.2.0

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
Merge pull request #1742 from PiranhaCMS/features/manager-security-up... · PiranhaCMS/piranha.core@e42abac · GitHub	github.com text/html	 MISC github.com/PiranhaCMS/piranha.core/commit/e42abacdd0dd880ce9cfe

CVE-2021-25976 | WhiteSource Vulnerability Database [www.whitesourcesoftware.com](https://www.whitesourcesoftware.com/text/html)  MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2021-25976

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.

980102 Dotnet (nuget) Security Update for Piranha (GHSA-ppq7-88c7-q879)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dotnetfoundation	Piranha Cms	4.0.0	-	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha1	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha3	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha4	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha5	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha6	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha7	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha8	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	alpha9	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	beta1	All	All
Application	Dotnetfoundation	Piranha Cms	4.0.0	rc1	All	All
Application	Dotnetfoundation	Piranha Cms	All	All	All	All

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:-:*:*:*:*:
```

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha1:*.:*:*:*.*
```

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha3:*:*:*:*:*
```

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha4:*:*:*:*:
```

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha5:*.**:*.**:*
```

```
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha6:*:*:*:*:
```

cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha7:~::~::~:
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha8:~::~::~:
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:alpha9:~::~::~:
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:beta1:~::~::~:
cpe:2.3:a:dotnetfoundation:piranha_cms:4.0.0:rc1:~::~::~:
cpe:2.3:a:dotnetfoundation:piranha_cms:~::~::~:

Discovery Credit

WhiteSource Vulnerability Research Team (WVR)

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-25976 : In PiranhaCMS, versions 4.0.0-alpha1 to 9.2.0 are vulnerable to cross-site request forgery CSRF... twitter.com/i/web/status/1...	2021-11-16 09:11:10

[← 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](#)