

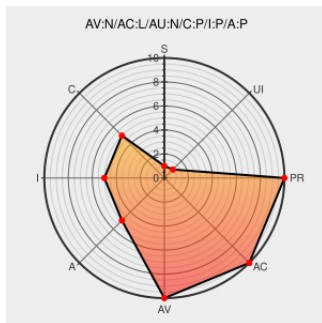


CVE-2006-4559

Published on: 09/05/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:56 PM UTC

CVE-2006-4559

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

Certain versions of [Yet Another Community System Cms](#) from [Bernard Pacques](#) contain the following vulnerability:

Multiple PHP remote file inclusion vulnerabilities in Yet Another Community System (YACS) CMS 6.6.1 allow remote attackers to execute arbitrary PHP code via a URL in the context[path_to_root] parameter in (1) articles/populate.php, (2) categories/category.php, (3) categories/populate.php, (4) comments/populate.php, (5) files/file.php, (6) sections/section.php, (7) sections/populate.php, (8) tables/populate.php, (9) users/user.php, and (10) users/populate.php. The articles/article.php vector is covered by CVE-2006-4532.

CVE-2006-4559 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

[www.osvdb.org](#)

[OSVDB 31310](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 31303](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 31304](#)

Inactive Link Not Archived

	Inactive Link Not Archived	
YACS "context[path_to_root]" File Inclusion Vulnerabilities - Advisories - Secunia	Exploit Patch Vendor Advisory web.archive.org text/html	SECUNIA 21680
Security Patch for YACS 6.6.1 - Yet Another Community System	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM www.yetanothercommunitysystem.com/yacs/articles/view.php/1664
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31308
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31301
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31306
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31305
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31302
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31307
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 31309

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	Bernard Pacques	Yet Another Community System Cms	6.6.1	All	All	All
Application	Bernard Pacques	Yet Another Community System Cms	6.6.1	All	All	All
cpe:2.3:a:bernard_pacques:yet_another_community_system_cms:6.6.1:*****:*						
cpe:2.3:a:bernard_pacques:yet_another_community_system_cms:6.6.1:*****:*						

No vendor comments have been submitted for this CVE

© [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](#)