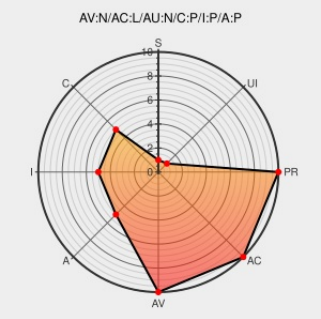
CVE-2014-2921

Published on: 04/21/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:57 PM UTC

CVE-2014-2921

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pimcore from Pimcore contain the following vulnerability:

The getObjectByToken function in Newsletter.php in the Pimcore_Tool_Newsletter module in pimcore 1.4.9 through 2.0.0 does not properly handle an object obtained by unserializing Lucene search data, which allows remote attackers to conduct PHP object injection attacks and execute arbitrary code via vectors involving a Zend_Pdf_ElementFactory_Proxy object and a pathname with a trailing \0 character.

CVE-2014-2921 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: Remote code execution in Pimcore CMS	openwall.com text/html	MLIST [oss-security] 20140421 Re: Remote code execution in Pimcore CMS
Page not found · GitHub · GitHub	Exploit github.com text/html Inactive Link Not Archived	MISC github.com/pedrib/PoC/blob/master/pimcore-2.1.0.txt
pimcore 2.2 released	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM www.pimcore.org/en/resources/blog/pimcore+2.2+released_b442

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.

Related QID Numbers

994887 PHP (Composer) Security Update for pimcore/pimcore (GHSA-g7pj-3v97-3vxp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pimcore	Pimcore	1.4.9	All	All	All
Application	Pimcore	Pimcore	1.5.0	All	All	All
Application	Pimcore	Pimcore	2.1.0	All	All	All
Application	Pimcore	Pimcore	2.2.0	All	All	All
Application	Pimcore	Pimcore	1.4.9	All	All	All
Application	Pimcore	Pimcore	1.5.0	All	All	All
Application	Pimcore	Pimcore	2.1.0	All	All	All
Application	Pimcore	Pimcore	2.2.0	All	All	All

cpe:2.3:a:pimcore:pimcore:1.4.9:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:1.5.0:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:2.1.0:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:2.2.0:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:1.4.9:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:1.5.0:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:2.1.0:*:*:*:*:*:*:*

cpe:2.3:a:pimcore:pimcore:2.2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report