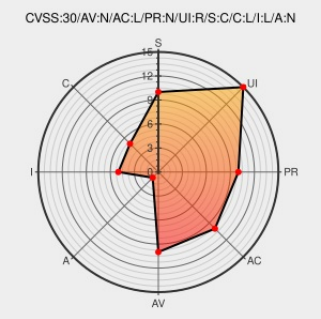
CVE-2018-1999016

Published on: 07/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-1999016

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



Certain versions of Pydio from Pydio contain the following vulnerability:

Pydio version 8.2.0 and earlier contains a Cross Site Scripting (XSS) vulnerability in ./core/vendor/meenie/javascript-packer/example-inline.php line 48; ./core/vendor/dapphp/securimage/examples/test.mysql.static.php lines: 114,118 that can result in an unauthenticated remote attacker manipulating the web client via XSS code injection. This attack appear to be exploitable via the victim openning a specially crafted URL. This vulnerability appears to have been fixed in version 8.2.1.

CVE-2018-1999016 has been assigned by 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
	Exploit	MISC www.mike-gualtieri.com/files/Pydio-8-VulnerabilityDisclosure

	Exploit Third Party Advisory www.mike-gualtieri.com text/plain	MISC www.mike-gualtieri.com/files/Pydio-8-VulnerabilityDisclosure-Jul18.txt
Pydio 8.2.1 - Security Release | Pydio	Patch Release Notes Vendor Advisory pydio.com text/html	CONFIRM pydio.com/en/community/releases/pydio-core/pydio-821-security-release

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pydio	Pydio	All	All	All	All

cpe:2.3:a:pydio:pydio:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→