



CVE-2013-4267

Published on: 02/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4267

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

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



Certain versions of [Pydio](#) from [Pydio](#) contain the following vulnerability:

Ajaxplorer before 5.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) archive_name parameter to the Power FS module

(plugins/action.powerfs/class.PowerFSController.php), a (2) file name to the getTrustSizeOnFileSystem function in the File System

(Standard) module (plugins/access.fs/class.fsAccessWrapper.php), or

the (3) revision parameter to the Subversion Repository module

(plugins/meta.svn/class.SvnManager.php).

CVE-2013-4267 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Call cexecshell() where missing	CVE-2013-4267	https://github.com/pydio/pydio

Call escapesnriarg where missing · pydio/pydio-core@22a6284 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/pydio/pydio-core/commit/22a62840e5ac14bb389
oss-security - Re: CVE requests for Ajaxplorer	Mailing List Third Party Advisory www.openwall.com text/html	 MISC www.openwall.com/lists/oss-security/2013/08/21/16
AjaXplorer < 5.0.1 Multiple Command Execution Vulnerabilities Tenable®	Third Party Advisory www.tenable.com text/html	 MISC www.tenable.com/plugins/nessus/70495

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	Pydio	Pydio	All	All	All	All
Application	Pydio	Pydio	All	All	All	All
cpe:2.3:a:pydio:pydio:*.***.***.*						
cpe:2.3:a:pydio:pydio:*.***.***.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)