



CVE-2018-1229

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1229
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-21 20:29:00 UTC
Updated	2019-10-09 23:38:00 UTC
Description	Pivotal Spring Batch Admin, all versions, contains a stored XSS vulnerability in the file upload feature. An unauthenticated r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pivotal Software	Spring Batch Admin	All	All	All	All
Application	Pivotal Software	Spring Batch Admin	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2018-1229: Stored XSS in file upload of Spring Batch Admin Security Pivotal	CONFIRM	pivotal.io	Vendor Adviso
Pivotal Spring Batch Admin CVE-2018-1229 HTML Injection Vulnerability	BID	www.securityfocus.com	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[996907](#) Java (Maven) Security Update for org.springframework.batch:spring-batch-admin-manager (GHSA-4cj8-779h-r25h)

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](#).

Free CVE JSON API cve.report/api

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