



CVE-2011-4103

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

Summary

CVE	CVE-2011-4103
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-27 01:55:00 UTC
Updated	2014-12-18 15:35:00 UTC
Description	emitters.py in Django Piston before 0.2.3 and 0.2.x before 0.2.2.1 does not properly deserialize YAML data, which allows re

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Djangoproject	Piston	All	All	All	All

References

Reference

- Bug 750658 – CVE-2011-4103 django-piston: vulnerability in de-serialization of YAML post data could possibly allow remote execution or arbitrary code execution
- 404 — Bitbucket
- Debian -- Security Information -- DSA-2344-1 python-django-piston
- Django | Weblog | Piston and Tastypie security releases issued
- oss-security - Re: CVE request for Django-piston and Tastypie
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

983497 Python (pip) Security Update for django-piston (GHSA-pvhp-v9qp-xf5r)

© [CVE.report](#) 2026 |

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](#)