



# CVE-2013-4192

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-4192
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-03-11 19:37:02 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	sendto.py in Plone 2.1 through 4.1, 4.2.x through 4.2.5, and 4.3.x through 4.3.1 allows remote authenticated users to spoof

## Risk And Classification

**Primary CVSS:** v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:P/A:N

**Problem Types:** CWE-20 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:S/C:N/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plone	Plone	2.1	All	All	All

Application	Plone	Plone	2.1.1	All	All	All
Application	Plone	Plone	2.1.2	All	All	All
Application	Plone	Plone	2.1.3	All	All	All
Application	Plone	Plone	2.1.4	All	All	All
Application	Plone	Plone	2.5	All	All	All
Application	Plone	Plone	2.5.1	All	All	All
Application	Plone	Plone	2.5.2	All	All	All
Application	Plone	Plone	2.5.3	All	All	All
Application	Plone	Plone	2.5.4	All	All	All
Application	Plone	Plone	2.5.5	All	All	All
Application	Plone	Plone	3.0	All	All	All
Application	Plone	Plone	3.0.1	All	All	All
Application	Plone	Plone	3.0.2	All	All	All
Application	Plone	Plone	3.0.3	All	All	All
Application	Plone	Plone	3.0.4	All	All	All
Application	Plone	Plone	3.0.5	All	All	All
Application	Plone	Plone	3.0.6	All	All	All
Application	Plone	Plone	3.1	All	All	All
Application	Plone	Plone	3.1.1	All	All	All
Application	Plone	Plone	3.1.2	All	All	All
Application	Plone	Plone	3.1.3	All	All	All
Application	Plone	Plone	3.1.4	All	All	All
Application	Plone	Plone	3.1.5.1	All	All	All
Application	Plone	Plone	3.1.6	All	All	All
Application	Plone	Plone	3.1.7	All	All	All
Application	Plone	Plone	3.2	All	All	All
Application	Plone	Plone	3.2.1	All	All	All
Application	Plone	Plone	3.2.2	All	All	All
Application	Plone	Plone	3.2.3	All	All	All
Application	Plone	Plone	3.3	All	All	All
Application	Plone	Plone	3.3.1	All	All	All
Application	Plone	Plone	3.3.2	All	All	All
Application	Plone	Plone	3.3.3	All	All	All
Application	Plone	Plone	3.3.4	All	All	All
Application	Plone	Plone	3.3.5	All	All	All
Application	Plone	Plone	4.0	All	All	All

Application	Plone	Plone	4.0.1	All	All	All
Application	Plone	Plone	4.0.2	All	All	All
Application	Plone	Plone	4.0.3	All	All	All
Application	Plone	Plone	4.0.4	All	All	All
Application	Plone	Plone	4.0.5	All	All	All
Application	Plone	Plone	4.0.6.1	All	All	All
Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.2	All	All	All
Application	Plone	Plone	4.2.1	All	All	All
Application	Plone	Plone	4.2.2	All	All	All
Application	Plone	Plone	4.2.3	All	All	All
Application	Plone	Plone	4.2.4	All	All	All
Application	Plone	Plone	4.2.5	All	All	All
Application	Plone	Plone	4.3	All	All	All
Application	Plone	Plone	4.3.1	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source
oss-sec: Re: CVE Request -- Plone: 20130618 Hotfix (multiple vectors)	af854a3a-2127-422b-
Security vulnerability announcement: 20130618 - Multiple vectors — Plone CMS: Open Source Content Management	af854a3a-2127-422b-
978464 – (CVE-2013-4192) CVE-2013-4192 plone: Ability to spoof emails (sendto.py)	af854a3a-2127-422b-
Plone Hotfix 20130618 — Plone CMS: Open Source Content Management	af854a3a-2127-422b-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)