

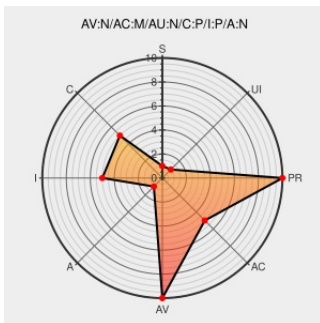


CVE-2013-4200

Published on: 01/21/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:45:00 AM UTC

CVE-2013-4200

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

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

The `isURLInPortal` method in the `URLTool` class in `in_portal.py` in [Plone](#) 2.1 through 4.1, 4.2.x through 4.2.5, and 4.3.x through 4.3.1 treats URLs starting with a space as a relative URL, which allows remote attackers to bypass the `allow_external_login_sites` filtering property, redirect users to arbitrary web sites, and conduct phishing attacks via a space before a URL in the "next" parameter to `acl_users/credentials_cookie_auth/require_login`.

CVE-2013-4200 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

oss-security - Re: CVE Request -- Plone: 20130618 Hotfix (multiple vectors)

www.openwall.com
[text/html](#)

[MLIST \[oss-security\] 20130801 Re: CVE Request -- Plone: 20130618 Hotfix \(multiple](#)

SecurityFocus

www.securityfocus.com
[text/html](#)

[BUGTRAQ 20140116 CVE-2013-4200 - Plone URL redirection / Forwarding of cookie data \(session hijack\) in certain browsers](#)

Security vulnerability announcement: 20130618 - Multiple vectors — Plone CMS: Open Source Content Management

[Vendor Advisory](#)
web.archive.org
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM](#)
plone.org/products/plone/security/advisories/20130618-announcement

Plone Hotfix 20130618 — Plone CMS: Open Source Content Management

[Patch](#)
web.archive.org

[CONFIRM](#) plone.org/products/plone-hotfix/releases/20130618

Content management

redhat.com

text/html

Inactive Link

Not Archived

978485 – (CVE-2013-4200) CVE-2013-4200 plone: Forwarding of cookie data (session hijack) in certain browsers (in_portal.py)

bugzilla.redhat.com

text/html

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2013-4200

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	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	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
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	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
cpe:2.3:a:plone:plone:2.1:*:*:*:*:*:						
cpe:2.3:a:plone:plone:2.1.1:*:*:*:*:*:						

cpe:2.3:a:plone:plone:2.1.2:*****:
cpe:2.3:a:plone:plone:2.1.3:*****:
cpe:2.3:a:plone:plone:2.1.4:*****:
cpe:2.3:a:plone:plone:3.0:*****:
cpe:2.3:a:plone:plone:3.0.1:*****:
cpe:2.3:a:plone:plone:3.0.2:*****:
cpe:2.3:a:plone:plone:3.0.3:*****:
cpe:2.3:a:plone:plone:3.0.4:*****:
cpe:2.3:a:plone:plone:3.0.5:*****:
cpe:2.3:a:plone:plone:3.0.6:*****:
cpe:2.3:a:plone:plone:3.1:*****:
cpe:2.3:a:plone:plone:3.1.1:*****:
cpe:2.3:a:plone:plone:3.1.2:*****:
cpe:2.3:a:plone:plone:3.1.3:*****:
cpe:2.3:a:plone:plone:3.1.4:*****:
cpe:2.3:a:plone:plone:3.1.5.1:*****:
cpe:2.3:a:plone:plone:3.1.6:*****:
cpe:2.3:a:plone:plone:3.1.7:*****:
cpe:2.3:a:plone:plone:3.2:*****:
cpe:2.3:a:plone:plone:3.2.1:*****:
cpe:2.3:a:plone:plone:3.2.2:*****:
cpe:2.3:a:plone:plone:3.2.3:*****:
cpe:2.3:a:plone:plone:3.3:*****:
cpe:2.3:a:plone:plone:3.3.1:*****:
cpe:2.3:a:plone:plone:3.3.2:*****:
cpe:2.3:a:plone:plone:3.3.3:*****:
cpe:2.3:a:plone:plone:3.3.4:*****:
cpe:2.3:a:plone:plone:3.3.5:*****:
cpe:2.3:a:plone:plone:4.0:*****:

cpe:2.3:a:plone:plone:4.0.*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.2:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.3:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.4:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.5:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.0.6.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2.2:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2.3:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2.4:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.2.5:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.3:*:*:*:*:*:
cpe:2.3:a:plone:plone:4.3.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:2.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:2.1.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:2.1.2:*:*:*:*:*:
cpe:2.3:a:plone:plone:2.1.3:*:*:*:*:*:
cpe:2.3:a:plone:plone:2.1.4:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.1:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.2:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.3:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.4:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.5:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.0.6:*:*:*:*:*:
cpe:2.3:a:plone:plone:3.1:*:*:*:*:*:

cpe:2.3:a:plone:plone:3.1.1:****:
cpe:2.3:a:plone:plone:3.1.2:****:
cpe:2.3:a:plone:plone:3.1.3:****:
cpe:2.3:a:plone:plone:3.1.4:****:
cpe:2.3:a:plone:plone:3.1.5.1:****:
cpe:2.3:a:plone:plone:3.1.6:****:
cpe:2.3:a:plone:plone:3.1.7:****:
cpe:2.3:a:plone:plone:3.2:****:
cpe:2.3:a:plone:plone:3.2.1:****:
cpe:2.3:a:plone:plone:3.2.2:****:
cpe:2.3:a:plone:plone:3.2.3:****:
cpe:2.3:a:plone:plone:3.3:****:
cpe:2.3:a:plone:plone:3.3.1:****:
cpe:2.3:a:plone:plone:3.3.2:****:
cpe:2.3:a:plone:plone:3.3.3:****:
cpe:2.3:a:plone:plone:3.3.4:****:
cpe:2.3:a:plone:plone:3.3.5:****:
cpe:2.3:a:plone:plone:4.0:****:
cpe:2.3:a:plone:plone:4.0.1:****:
cpe:2.3:a:plone:plone:4.0.2:****:
cpe:2.3:a:plone:plone:4.0.3:****:
cpe:2.3:a:plone:plone:4.0.4:****:
cpe:2.3:a:plone:plone:4.0.5:****:
cpe:2.3:a:plone:plone:4.0.6.1:****:
cpe:2.3:a:plone:plone:4.1:****:
cpe:2.3:a:plone:plone:4.2:****:
cpe:2.3:a:plone:plone:4.2.1:****:
cpe:2.3:a:plone:plone:4.2.2:****:

cpe:2.3:a:plone:plone:4.2.3:*****:
cpe:2.3:a:plone:plone:4.2.4:*****:
cpe:2.3:a:plone:plone:4.2.5:*****:
cpe:2.3:a:plone:plone:4.3:*****:
cpe:2.3:a:plone:plone:4.3.1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

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](#)