

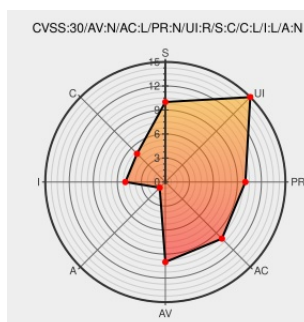


CVE-2017-1000481

Published on: 01/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000481

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

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

When you visit a page where you need to login, Plone 2.5-5.1rc1 sends you to the login form with a 'came_from' parameter set to the previous url. After you login, you get redirected to the page you tried to view before. An attacker might try to abuse this by letting you click on a specially crafted link. You would login, and get redirected to the site of the attacker, letting you think that you are still on the original Plone site.

Or some javascript of the attacker could be executed. Most of these types of attacks are already blocked by Plone, using the `isURLInPortal` check to make sure we only redirect to a page on the same Plone site. But a few more ways of tricking Plone into accepting a malicious link were discovered, and fixed with this hotfix.

CVE-2017-1000481 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

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				
Open redirection on login form — Plone.org	Vendor Advisory plone.org text/html	 MISC plone.org/security/hotfix/20171128/open-redirection-on-login-form				
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	2.5.5	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	3.3.6	All	All	All
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.0.1	All	All	All
Application	Plone	Plone	4.0.10	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	4.0.7	All	All	All
Application	Plone	Plone	4.0.8	All	All	All
Application	Plone	Plone	4.0.9	All	All	All
Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.1.1	All	All	All
Application	Plone	Plone	4.1.2	All	All	All
Application	Plone	Plone	4.1.3	All	All	All
Application	Plone	Plone	4.1.4	All	All	All
Application	Plone	Plone	4.1.5	All	All	All

Application	Plone	Plone	4.1.6	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	4.2.6	All	All	All
Application	Plone	Plone	4.2.7	All	All	All
Application	Plone	Plone	4.3	All	All	All
Application	Plone	Plone	4.3.1	All	All	All
Application	Plone	Plone	4.3.10	All	All	All
Application	Plone	Plone	4.3.11	All	All	All
Application	Plone	Plone	4.3.12	All	All	All
Application	Plone	Plone	4.3.14	All	All	All
Application	Plone	Plone	4.3.15	All	All	All
Application	Plone	Plone	4.3.2	All	All	All
Application	Plone	Plone	4.3.3	All	All	All
Application	Plone	Plone	4.3.4	All	All	All
Application	Plone	Plone	4.3.5	All	All	All
Application	Plone	Plone	4.3.6	All	All	All
Application	Plone	Plone	4.3.7	All	All	All
Application	Plone	Plone	4.3.8	All	All	All
Application	Plone	Plone	4.3.9	All	All	All
Application	Plone	Plone	5.0	All	All	All
Application	Plone	Plone	5.0	rc1	All	All
Application	Plone	Plone	5.0	rc2	All	All
Application	Plone	Plone	5.0	rc3	All	All
Application	Plone	Plone	5.0.1	All	All	All
Application	Plone	Plone	5.0.2	All	All	All
Application	Plone	Plone	5.0.3	All	All	All
Application	Plone	Plone	5.0.4	All	All	All
Application	Plone	Plone	5.0.5	All	All	All
Application	Plone	Plone	5.0.6	All	All	All
Application	Plone	Plone	5.0.7	All	All	All
Application	Plone	Plone	5.0.8	All	All	All

Application	Plone	Plone	5.0.9	All	All	All
Application	Plone	Plone	5.1	a1	All	All
Application	Plone	Plone	5.1	a2	All	All
Application	Plone	Plone	5.1	b2	All	All
Application	Plone	Plone	5.1	b3	All	All
Application	Plone	Plone	5.1	b4	All	All
Application	Plone	Plone	5.1	rc1	All	All
Application	Plone	Plone	2.5.5	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	3.3.6	All	All	All
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.0.1	All	All	All
Application	Plone	Plone	4.0.10	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	4.0.7	All	All	All
Application	Plone	Plone	4.0.8	All	All	All
Application	Plone	Plone	4.0.9	All	All	All
Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.1.1	All	All	All
Application	Plone	Plone	4.1.2	All	All	All
Application	Plone	Plone	4.1.3	All	All	All
Application	Plone	Plone	4.1.4	All	All	All
Application	Plone	Plone	4.1.5	All	All	All
Application	Plone	Plone	4.1.6	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	4.2.6	All	All	All
Application	Plone	Plone	4.2.7	All	All	All
Application	Plone	Plone	4.3	All	All	All
Application	Plone	Plone	4.3.1	All	All	All
Application	Plone	Plone	4.3.10	All	All	All
Application	Plone	Plone	4.3.11	All	All	All
Application	Plone	Plone	4.3.12	All	All	All
Application	Plone	Plone	4.3.14	All	All	All
Application	Plone	Plone	4.3.15	All	All	All
Application	Plone	Plone	4.3.2	All	All	All
Application	Plone	Plone	4.3.3	All	All	All
Application	Plone	Plone	4.3.4	All	All	All
Application	Plone	Plone	4.3.5	All	All	All
Application	Plone	Plone	4.3.6	All	All	All
Application	Plone	Plone	4.3.7	All	All	All
Application	Plone	Plone	4.3.8	All	All	All
Application	Plone	Plone	4.3.9	All	All	All
Application	Plone	Plone	5.0	All	All	All
Application	Plone	Plone	5.0	rc1	All	All
Application	Plone	Plone	5.0	rc2	All	All
Application	Plone	Plone	5.0	rc3	All	All
Application	Plone	Plone	5.0.1	All	All	All
Application	Plone	Plone	5.0.2	All	All	All
Application	Plone	Plone	5.0.3	All	All	All
Application	Plone	Plone	5.0.4	All	All	All
Application	Plone	Plone	5.0.5	All	All	All
Application	Plone	Plone	5.0.6	All	All	All
Application	Plone	Plone	5.0.7	All	All	All
Application	Plone	Plone	5.0.8	All	All	All
Application	Plone	Plone	5.0.9	All	All	All
Application	Plone	Plone	5.1	a1	All	All
Application	Plone	Plone	5.1	a2	All	All
Application	Plone	Plone	5.1	a3	All	All

Application	Plone	Plone	5.1	b2	All	All
Application	Plone	Plone	5.1	b3	All	All
Application	Plone	Plone	5.1	b4	All	All
Application	Plone	Plone	5.1	rc1	All	All
cpe:2.3:a:plone:plone:2.5.5:*****:						
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:3.3.6:*****:						
cpe:2.3:a:plone:plone:4.0:*****:						
cpe:2.3:a:plone:plone:4.0.1:*****:						
cpe:2.3:a:plone:plone:4.0.10:*****:						
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:4.0.7:*****:						
cpe:2.3:a:plone:plone:4.0.8:*****:						
cpe:2.3:a:plone:plone:4.0.9:*****:						
cpe:2.3:a:plone:plone:4.1:*****:						
cpe:2.3:a:plone:plone:4.1.1:*****:						
cpe:2.3:a:plone:plone:4.1.2:*****:						
cpe:2.3:a:plone:plone:4.1.3:*****:						
cpe:2.3:a:plone:plone:4.1.4:*****:						
cpe:2.3:a:plone:plone:4.1.5:*****:						
cpe:2.3:a:plone:plone:4.1.6:*****:						
cpe:2.3:a:plone:plone:4.2:*****:						

cpe:2.3:a:pione:pione: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:4.2.6:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:4.2.7:*:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:4.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.11:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.15:*:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:4.3.2:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:4.3.3:*:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:4.3.4:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.5:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.6:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:4.3.9:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:5.0:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:5.0:rc1:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:5.0:rc2:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:5.0:rc3:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:5.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:plone:plone:5.0.2:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:5.0.3:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.4:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.5:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.6:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.7:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.8:*:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.0.9:*:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:5.1:a1:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:5.1:a2:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.1:b2:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.1:b3:*:*:*:*:*:

cpe:2.3:a:plone:plone:5.1:b4:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:5.1:rc1:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:2.5.5:*:*:*:*:*:*:

```
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:3.3.6:*:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:4.0:*:*:*:*:*:*:
```

cpe:2.3:a:plone:plone:4.0.1:*:*:*:*:*:*:

```
cpe:2.3:a:plone:plone:4.0.10:*:*:*:*:*:*:*:
```

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:4.0.7:*****:
cpe:2.3:a:plone:plone:4.0.8:*****:
cpe:2.3:a:plone:plone:4.0.9:*****:
cpe:2.3:a:plone:plone:4.1:*****:
cpe:2.3:a:plone:plone:4.1.1:*****:
cpe:2.3:a:plone:plone:4.1.2:*****:
cpe:2.3:a:plone:plone:4.1.3:*****:
cpe:2.3:a:plone:plone:4.1.4:*****:
cpe:2.3:a:plone:plone:4.1.5:*****:
cpe:2.3:a:plone:plone:4.1.6:*****:
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:4.2.6:*****:
cpe:2.3:a:plone:plone:4.2.7:*****:
cpe:2.3:a:plone:plone:4.3:*****:
cpe:2.3:a:plone:plone:4.3.1:*****:
cpe:2.3:a:plone:plone:4.3.10:*****:
cpe:2.3:a:plone:plone:4.3.11:*****:
cpe:2.3:a:plone:plone:4.3.12:*****:
cpe:2.3:a:plone:plone:4.3.14:*****:
cpe:2.3:a:plone:plone:4.3.15:*****:
cpe:2.3:a:plone:plone:4.3.2:*****:
cpe:2.3:a:plone:plone:4.3.3:*****:
cpe:2.3:a:plone:plone:4.3.4:*****:
cpe:2.3:a:plone:plone:4.3.5:*****:

cpe:2.3:a:plone:plone:4.3.6:*****:
cpe:2.3:a:plone:plone:4.3.7:*****:
cpe:2.3:a:plone:plone:4.3.8:*****:
cpe:2.3:a:plone:plone:4.3.9:*****:
cpe:2.3:a:plone:plone:5.0:*****:
cpe:2.3:a:plone:plone:5.0:rc1:*****:
cpe:2.3:a:plone:plone:5.0:rc2:*****:
cpe:2.3:a:plone:plone:5.0:rc3:*****:
cpe:2.3:a:plone:plone:5.0.1:*****:
cpe:2.3:a:plone:plone:5.0.2:*****:
cpe:2.3:a:plone:plone:5.0.3:*****:
cpe:2.3:a:plone:plone:5.0.4:*****:
cpe:2.3:a:plone:plone:5.0.5:*****:
cpe:2.3:a:plone:plone:5.0.6:*****:
cpe:2.3:a:plone:plone:5.0.7:*****:
cpe:2.3:a:plone:plone:5.0.8:*****:
cpe:2.3:a:plone:plone:5.0.9:*****:
cpe:2.3:a:plone:plone:5.1:a1:*****:
cpe:2.3:a:plone:plone:5.1:a2:*****:
cpe:2.3:a:plone:plone:5.1:b2:*****:
cpe:2.3:a:plone:plone:5.1:b3:*****:
cpe:2.3:a:plone:plone:5.1:b4:*****:
cpe:2.3:a:plone:plone:5.1:rc1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

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](#)