

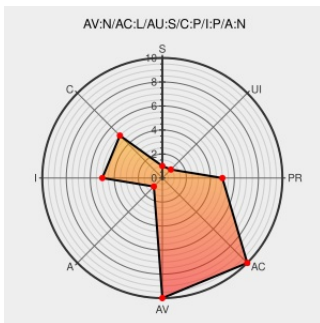


CVE-2013-7061

Published on: 05/02/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7061

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

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

Products/CMFPlone/CatalogTool.py in Plone 3.3 through 4.3.2 allows remote administrators to bypass restrictions and obtain sensitive information via an unspecified search API.

CVE-2013-7061 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

oss-security - Re: CVE request for Plone

[www.openwall.com](http://www.openwall.com/text/html)
text/html

[MLIST \[oss-security\] 20131211 Re: CVE request for Plone](#)

Privilege escalation through exposed underlying API — Plone CMS: Open Source Content Management

[Vendor Advisory](#)
[plone.org](http://plone.org/text/html)
text/html

[CONFIRM](#)
plone.org/security/20131210/catalogue-exposure

oss-security - CVE request for Plone

[www.openwall.com](http://www.openwall.com/text/html)
text/html

[MLIST \[oss-security\] 20131210 CVE request for Plone](#)

By selecting these links, you may be leaving CVEreport workspace. 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	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	4.0.2	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	4.0.9	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

УРЕ.З.У.А.ПЮИТЕ.ПЮИТЕ.У.У.

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:4.0.2:*:*:*:*:*:*:
```

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:4.0.9:*:*:*:*:*:*:
```

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:4.3.2:*:*:*:*:*:*:

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:4.0.2:*:*:*:*:*:*:

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:4.0.9:*:*:*:*:*:*:
```

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:4.3.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)