



# CVE-2015-8483

Published on: 02/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

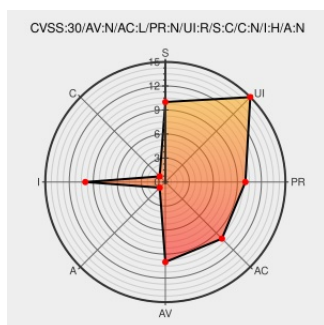
## CVE-2015-8483

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Open redirect vulnerability in Cybozu Office 10.2.0 through 10.3.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a crafted URL.

CVE-2015-8483 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.4 - HIGH**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **5.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                                | Tags                                                                                            | Link                                                                        |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 特定の機能でオープンリダイレクトの脆弱性【CyVDB-785】（2015/12/14）   サイボウズからのお知らせ | <a href="#">Vendor Advisory</a><br><a href="#">cs.cybozu.co.jp</a><br><a href="#">text/html</a> | <a href="#">CONFIRM</a><br><a href="#">cs.cybozu.co.jp/2015/006088.html</a> |
| JVN#71428831: Cybozu Office vulnerable to open redirect    | <a href="#">Vendor Advisory</a>                                                                 | <a href="#">JVN JVN#71428831</a>                                            |

[jvn.jp](#)[text/xml](#)

No Description Provided

Vendor Advisory

 JVND JVND-2016-000025[jvndb.jvn.jp](#)[text/html](#)

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](mailto: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 | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.1  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.2  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.1.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.1.2  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.2.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.3.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.0     | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.1.0   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.2.0   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.2.1   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.3.0   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.3.1   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.3.2   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.9.0   | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.1  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.0.2  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.1.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.1.2  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.2.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 10.3.0  | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.0     | All    | All     | All      |
| Application | <a href="#">Cybozu</a> | <a href="#">Office</a> | 9.1.0   | All    | All     | All      |

|                                       |        |        |       |     |     |     |
|---------------------------------------|--------|--------|-------|-----|-----|-----|
| Application                           | Cybozu | Office | 9.2.0 | All | All | All |
| Application                           | Cybozu | Office | 9.2.1 | All | All | All |
| Application                           | Cybozu | Office | 9.3.0 | All | All | All |
| Application                           | Cybozu | Office | 9.3.1 | All | All | All |
| Application                           | Cybozu | Office | 9.3.2 | All | All | All |
| Application                           | Cybozu | Office | 9.9.0 | All | All | All |
| cpe:2.3:a:cybozu:office:10.0.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.0.1:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.0.2:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.1.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.1.2:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.2.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.3.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.0:*****:    |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.1.0:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.2.0:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.2.1:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.3.0:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.3.1:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.3.2:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.9.0:*****:  |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.0.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.0.1:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.0.2:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.1.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.1.2:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.2.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:10.3.0:*****: |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.0:*****:    |        |        |       |     |     |     |
| cpe:2.3:a:cybozu:office:9.1.0:*****:  |        |        |       |     |     |     |

|                                        |
|----------------------------------------|
| cpe:2.3:a:cybozu:office:9.2.0:~::~::~: |
| cpe:2.3:a:cybozu:office:9.2.1:~::~::~: |
| cpe:2.3:a:cybozu:office:9.3.0:~::~::~: |
| cpe:2.3:a:cybozu:office:9.3.1:~::~::~: |
| cpe:2.3:a:cybozu:office:9.3.2:~::~::~: |
| cpe:2.3:a:cybozu:office:9.9.0:~::~::~: |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→