



# CVE-2018-6871

Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

## CVE-2018-6871

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

LibreOffice before 5.4.5 and 6.x before 6.0.1 allows remote attackers to read arbitrary files via =WEBSERVICE calls in a document, which use the COM.MICROSOFT.WEBSERVICE function.

CVE-2018-6871 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **5 - MEDIUM**

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

## CVE References

| Description                                                                                                                                    | Tags                                                                                                                       | Link                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| GitHub - jollheef/libreoffice-remote-arbitrary-file-disclosure: Proof of concept of LibreOffice remote arbitrary file disclosure vulnerability | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/jollheef/libreoffice-remote-arbitrary-file-disclosure</a> |

|                                                                                            |                                                                                                                                                                                                     |                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| USN-3579-1: LibreOffice vulnerability   Ubuntu security notices                            | <a href="#">Third Party Advisory</a><br><a href="#">usn.ubuntu.com</a><br><a href="#">text/html</a>                                                                                                 |  UBUNTU USN-3579-1                                                                                                                             |
| Red Hat Customer Portal                                                                    | <a href="#">Third Party Advisory</a><br><a href="#">access.redhat.com</a><br><a href="#">text/html</a>                                                                                              |  REDHAT RHSA-2018:0517                                                                                                                        |
| libreoffice/core - main, development code repository                                       | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">cgit.freedesktop.org</a><br><a href="#">text/html</a>                                                                  |  CONFIRM<br><a href="#">cgit.freedesktop.org/libreoffice/core/commit/?h=libreoffice-5-4-5&amp;id=a916fc0c0e0e8b10cb4158fa0fa173fe205d434a</a> |
| CVE-2018-6871   LibreOffice - Free Office Suite - Fun Project - Fantastic People           | <a href="#">Vendor Advisory</a><br><a href="#">www.libreoffice.org</a><br><a href="#">text/html</a>                                                                                                 |  CONFIRM <a href="#">www.libreoffice.org/about-us/security/advisories/cve-2018-1055/</a>                                                      |
| LibreOffice < 6.0.1 - 'WEBSERVICE' Remote Arbitrary File Disclosure - Linux remote Exploit | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">www.exploit-db.com</a><br><a href="#">Proof of Concept</a><br><a href="#">text/html</a> |  EXPLOIT-DB 44022                                                                                                                             |
| Debian -- Security Information -- DSA-4111-1 libreoffice                                   | <a href="#">Third Party Advisory</a><br><a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a>                                                              |  DEBIAN DSA-4111                                                                                                                              |
| Red Hat Customer Portal                                                                    | <a href="#">Third Party Advisory</a><br><a href="#">access.redhat.com</a><br><a href="#">text/html</a>                                                                                              |  REDHAT RHSA-2018:0418                                                                                                                       |

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).

## Related QID Numbers

[710254](#) Gentoo Linux LibreOffice Information disclosure Vulnerability (GLSA 201802-06)

## Known Affected Configurations (CPE V2.3)

| Type             | Vendor                    | Product                      | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 17.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 17.10   | All    | All     | All      |

|                  |             |                             |       |        |     |     |
|------------------|-------------|-----------------------------|-------|--------|-----|-----|
| Operating System | Debian      | Debian Linux                | 9.0   | All    | All | All |
| Operating System | Debian      | Debian Linux                | 9.0   | All    | All | All |
| Application      | Libreoffice | Libreoffice                 | All   | All    | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | All    | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | alpha1 | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | beta1  | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | beta2  | All | All |
| Application      | Libreoffice | Libreoffice                 | All   | All    | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | All    | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | alpha1 | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | beta1  | All | All |
| Application      | Libreoffice | Libreoffice                 | 6.0.0 | beta2  | All | All |
| Operating System | Redhat      | Enterprise Linux Desktop    | 6.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Desktop    | 7.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Desktop    | 6.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Desktop    | 7.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server     | 6.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server     | 7.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server     | 6.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server     | 7.0   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Aus | 7.4   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Aus | 7.6   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Aus | 7.4   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Aus | 7.6   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Eus | 7.4   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Eus | 7.5   | All    | All | All |
| Operating System | Redhat      | Enterprise Linux Server Eus | 7.6   | All    | All | All |



|                                                              |
|--------------------------------------------------------------|
| cpe:2.3:a:libreoffice:libreoffice:6.0.0:*:*:*:*:*:           |
| cpe:2.3:a:libreoffice:libreoffice:6.0.0:alpha1:*:*:*:*:      |
| cpe:2.3:a:libreoffice:libreoffice:6.0.0:beta1:*:*:*:*:       |
| cpe:2.3:a:libreoffice:libreoffice:6.0.0:beta2:*:*:*:*:       |
| cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:     |
| cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:      |
| cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:      |
| cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:      |
| cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:      |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.4:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*: |

cpe:2.3:o:redhat:enterprise\_linux\_workstation:7.0:\*:\*:\*:\*:\*:

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](#)