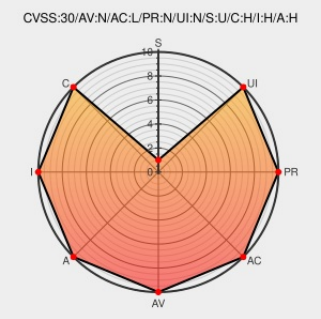
CVE-2018-6871

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 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
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GitHub - jollheef/libreoffice-remote-arbitrary-file-disclosure: Proof of concept of LibreOffice remote arbitrary file disclosure vulnerability	Exploit, Third Party Advisory, github.com, text/html	MISC github.com/jollheef/libreoffice-remote-arbitrary-file-disclosure

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

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	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	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

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
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:libreoffice:libreoffice:*:*:*:*:*:*:*:*:

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:a:libreoffice:libreoffice:*:*:*:*:*:*:*:*:

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→