



Lack of Throttling on Email Functionality

#PT12068 4

Pending Fix

Low

· Server Security Misconfiguration · Aug 11, 2022

(pranavhivar...)

Vulnerability Type

Server Security Misconfiguration > No Rate Limiting on Form > Email-Triggering

Description

The software does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests.

This can allow the actor to perform actions more frequently than expected. The actor could be a human or an automated process such as a virus or bot. This could be used to cause a denial of service, compromise program logic (such as limiting humans to a single vote), or other consequences. For example, an authentication routine might not limit the number of times an attacker can guess a password. Or, a web site might conduct a poll but only expect humans to vote a maximum of once a day.

The email functionality of the <https://pentest.beta.nuxeocloud.com/> application is not throttled when a user sends out notification emails. This allows an attacker to use the forge web application to send excessive mail volume to unsuspecting people.

Affected URL(s)

```
https://pentest.beta.nuxeocloud.com/nuxeo/ui/#!/browse/default-domain/sections/test.html?p=permissions
```

Proof of Concept

1] Login into your admin account on <https://pentest.beta.nuxeocloud.com>

2] Create a file and go to the permissions tab.

Eg. <https://pentest.beta.nuxeocloud.com/nuxeo/ui/#!/browse/default-domain/sections/test.html?p=permissions>

3] Now, share the file with an external user and add

email

and your message to be sent in email. Click

Send email

from

Actions

as shown in image.

The screenshot shows a web browser interface for a document titled 'test.html'. The URL is <https://pentest.beta.nuxeocloud.com/nuxeo/ui/#i/browse/default-domain/sections/test.html?p=permissions>. The page is divided into three main sections:

- Permissions defined locally:** A section with a 'New' button and the text 'There are no local permissions.'
- Permissions inherited from upper levels:** A section with a 'Block' button and a paragraph explaining inheritance control. Below it is a table with the following data:

User / Group	Right	Time Frame	Granted by
members	canAskForPublishing	Permanent	
Administrator	Manage everything	Permanent	
members	Read	Permanent	
- Permissions Assigned to External Users:** A section with a 'New' button and a paragraph explaining external user sharing. Below it is a table with the following data:

User / Group	Right	Time Frame	Granted by	Actions
phivarekar+test@cobaltcore.io	Read	Since 11 Aug 2022 until 31 Aug 2022	pentest-admin	[Edit] [Share] [Delete]

4] Intercept the request and send it to the intruder and repeat for many times. It will send that many emails to the user.

Attack Save Columns 3. Intruder attack of pentest.beta.nuxeocloud.com - Temporary attack - Not saved to project file

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
250	250	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
249	249	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
248	248	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
247	247	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
244	244	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
243	243	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
242	242	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
241	241	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
240	240	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
239	239	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
238	238	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
237	237	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	
236	236	200	<input type="checkbox"/>	<input type="checkbox"/>	2897	

Request Response

Pretty Raw Hex Render \n

```

1 HTTP/1.1 200
2 Date: Thu, 11 Aug 2022 16:24:19 GMT
3 Content-Type: application/json; nuxeo-entity=document
4 Connection: close
5 Set-Cookie: AWSALB=Zmwg1X5F3EhJXKjMmXwy8ruu+TFBhkZ7NUd1+hbsOUKNr8jxz zva6 iRxxhEU2UMHSKjh6EKGoRXHATWo7+cmOxmrcVa20BUUVI
6 Set-Cookie: AWSALBCORS=Zmwg1X5F3EhJXKjMmXwy8ruu+TFBhkZ7NUd1+hbsOUKNr8jxz zva6 iRxxhEU2UMHSKjh6EKGoRXHATWo7+cmOxmrcVa20I
7 Server: Apache
8 Referrer-Policy: same-origin
9 Strict-Transport-Security: max-age=63072000; includeSubdomains;
10 X-Frame-Options: SAMEORIGIN
11 Referrer-Policy: strict-origin-when-cross-origin
12 X-UA-Compatible: IE=10; IE=11
13 Cache-Control: no-cache
14 X-Content-Type-Options: nosniff
15 Content-Security-Policy: img-src data: blob: *; default-src blob: *; script-src 'unsafe-inline' 'unsafe-eval' data:
16 X-XSS-Protection: 1; mode=block
    
```

0 matches

249 of 250

<input type="checkbox"/>	☆	nxsec-bounty-no-r...	30	"nxsec-bounty" New permission on test.html - Nuxeo Platform You now have ...	9:54 PM
<input type="checkbox"/>	☆	nxsec-bounty-no-r...	100	"nxsec-bounty" New permission on test.html - Nuxeo Platform You now have ...	9:53 PM
<input type="checkbox"/>	☆	nxsec-bounty-no-r...	100	"nxsec-bounty" New permission on test.html - Nuxeo Platform You now have ...	9:51 PM

Severity

All users of the application are vulnerable to this vulnerability. An attacker needs a victim's valid email address to flood the victim inbox, which can harm the Nuxeo's reputation.

Suggested Fix

1. Use a
 2. **CAPTCHA**

to limit email triggering requests.
3. Use a rate limit per IP address to throttle the amount of email triggering requests that can be made in a certain amount of time.

HTTP Request

```
POST /nuxeo/api/v1/automation/
Document.SendNotificationEmailForPermission HTTP/1.1
Host: pentest.beta.nuxeocloud.com
Cookie: JSESSIONID=9AD55F87B462297FAA8C94DD3DD2C6A7.nuxeo;
AWSALB=BC79j20BcH4t000zuxMuj7ZmFFWwMI/
u+hjoLDwyn4sys9ZHicNteWi6xAU4s2Bry4HNdk0RaDr0vyrW/
MN0lbLkUnB5Ma4gnf8ho2q8IXLSYcSoeNIHgyvuzz+v;
AWSALBCORS=BC79j20BcH4t000zuxMuj7ZmFFWwMI/
u+hjoLDwyn4sys9ZHicNteWi6xAU4s2Bry4HNdk0RaDr0vyrW/
MN0lbLkUnB5Ma4gnf8ho2q8IXLSYcSoeNIHgyvuzz+v;
org.jboss.seam.core.TimeZone=Asia/Kolkata;
nuxeo.start.url.fragment=!%2Fadmin%2Fanalytics
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0)
Gecko/20100101 Firefox/103.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Content-Type: application/json
Content-Length: 171
Properties: *
X-Nxrepository: default
Origin: https://pentest.beta.nuxeocloud.com
Sec-Fetch-Dest: 103
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://pentest.beta.nuxeocloud.com/nuxeo/ui/
Te: trailers
Connection: close
```

```
{"params":{"id":"transient/
phivarekar+test@cobaltcore.io:Read:true:pentest-
admin:1660156200000:1661884200000"},"context":{},"input":"d79a30e2-
80e8-466b-b258-4a21fff0b0f0"}
```