

# V-SOL GPON/EPON OLT Platform 2.03 Link Manipulation

2019.09.30		
Credit: <a href="https://cxsecurity.com/author/LiquidWorm/1/">LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)</a>		
Risk: <input type="text" value="Low"/>	Local: <input type="text" value="No"/>	Remote: <input type="text" value="Yes"/>
CVE: <input type="text" value="N/A"/>	CWE: <input type="text" value="N/A"/>	

**V-SOL GPON/EPON OLT Platform v2.03 Link Manipulation Vulnerability**

**Vendor:** Guangzhou V-SOLUTION Electronic Technology Co., Ltd.  
**Product web page:** <https://www.vsolcn.com>  
**Affected version:** V2.03.62R\_IPv6  
V2.03.54R  
V2.03.52R  
V2.03.49  
V2.03.47  
V2.03.40  
V2.03.26  
V2.03.24  
V1.8.6  
V1.4

**Summary:** GPON is currently the leading FTTH standard in broadband access technology being widely deployed by service providers around the world. GPON/EPON OLT products are 1U height 19 inch rack mount products. The features of the OLT are small, convenient, flexible, easy to deploy, high

performance. It is appropriate to be deployed in compact room environment.

The OLTs can be used for 'Triple-Play', VPN, IP Camera, Enterprise LAN and ICT applications.

Desc: Input passed via the 'parent' GET parameter in 'bindProfile.html' script

is not properly verified before being used to redirect users. This can be

exploited to redirect a logged-in user to an arbitrary website e.

g. when a

user clicks a specially crafted link to the affected script hosted on a trusted

domain.

Tested on: GoAhead-Webs

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic  
@zeroscience

Advisory ID: ZSL-2019-5535

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5535.php>

25.09.2019

--

CSRF URL Redirect request:

GET /action/bindProfile.html?parent=https://zeroscience.mk/index

Host: 192.168.8.200

Response:


HTTP/1.1 200 OK


Location: <https://zeroscience.mk/index.html?select=0>

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2019090193>)

Post

Vote for this issue:

 0

 -1

0%

100%

### Comment it here.


Nick (\*)

Email (\*)

Video


Text (\*)



**localheartzzz**  | Date: 2019-10-01 06:24 CET+1

This same open redirect vulnerability?



**jp\_localhost**  | Date: 2021-04-24 06:22 CET+1

Is this issue over? still, having this issue?

Copyright **2026**, cxsecurity.com