

V-SOL GPON/EPON OLT Platform 2.03 Cross Site Scripting

2019.09.30

Credit: [LiquidWorm \(https://cxsecurity.com/author/LiquidWorm/1/\)](https://cxsecurity.com/author/LiquidWorm/1/)

Risk: **Low**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-79**
(<https://cxsecurity.com/cwe/CWE-79>)

V-SOL GPON/EPON OLT Platform v2.03 Reflected XSS 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 deplo

y, 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: The application is prone to multiple reflected cross-site scripting vulnerabilities due to a failure to properly sanitize user-supplied input to several parameters that are handled by various scripts. Attackers can exploit this issue to execute arbitrary HTML and script code in a user's browser session.

Tested on: GoAhead-Webs

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2019-5537

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5537.php>

25.09.2019

--

```
GET /action/bindProfile.html?parent=""><script>confirm(251)</script>
>&gponid=2&gonuid=7
GET /action/ntp.html?sntp_en=1&time_zone=05%3A30&sntp_server=""><script>confirm(251)</script>&who=0
```

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2019090194>)

Post

Vote for this issue:

50% 50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)