

Yahei-PHP Prober 0.4.7 HTML Injection

2019.07.27

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

Risk: Low

Local: No

Remote: Yes

CVE: N/A

CWE: N/A

Yahei-PHP Prober v0.4.7 (speed) Remote HTML Injection Vulnerability

Vendor: Yahei.Net

Product web page: <http://www.yahei.net>

Affected version: 0.4.7

Summary: Detection of system web server operating environment.

Desc: Input passed to the GET parameter 'speed' is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML code in a user's browser session in context of an affected site.

/prober.php:

```
206: elseif(isset($_GET['speed']) and $_GET['speed']>0)
207: {
208:     $speed=round(100/($_GET['speed']/1000),2); //下载速度: $speed kb/s
```

```

209: }
...
...
1393:  <?php echo (isset($_GET['speed']))?"Download 1000KB Used <
font color='#cc0000'>".$_GET['speed']."</font> Millisecond, Downlo
ad Speed: "."<font color='#cc0000'>".$_speed."</font>"." kb/s":"<fo
nt color='#cc0000'>&nbsp;No Test&nbsp;</font>" ?>

```

```

-----
-----

```

Tested on: OneinStack (Linux 3.10.0-862.14.4.el7.x86_64)
nginx/1.14.0
PHP/7.2.11

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2019-5531
Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5531.php>

16.07.2019

--


PoC:

<http://domain.local:80/prober.php?speed=<marquee>marq</marquee>>

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2019070132>)

Post

Vote for this issue:

 0	 0
50%	50%

Comment it here.

Nick (*)

Email (*)

Video

Text (*)