WEMS Enterprise Manager 2.58 Cross Site Scripting

2020.01.05

Credit: **LiquidWorm (https://cxsecurity.com/author/LiquidWorm/1/)**

Risk: **Low** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

```
WEMS Enterprise Manager 2.58 (email) Reflected XSS


Vendor: WEMS Limited
Product web page: https://www.wems.co.uk
Affected version: 2.58.8903
                  2.55.8806
                  2.55.8782
                  2.19.7959

Summary: WEMS Enterprise Manager is a centralised management and monitoring
system for many WEMS equipped sites. It retrieves and stores data to enable
energy analysis at an enterprise wide level. It is designed to give global
visibility of the key areas that affect a buildings' environmental and energy
performance using site data collected via WEMS Site Managers or Niagara compatible
hardware.

Desc: Input passed to the GET parameter 'email' 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.

Tested on: Linux
           PHP


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2019-5551
Advisory URL: https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5551.php


06.07.2019

--


https://192.168.1.244/guest/users/forgotten?email="><script>confirm(251)</script>
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020010032)

Tw | Lul

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)