WEMS Enterprise Manager 2.58 (email) Reflected XSS

Title: WEMS Enterprise Manager 2.58 (email) Reflected XSS
Advisory ID: ZSL-2019-5551
Type: Local/Remote
Impact: Cross-Site Scripting
Risk: (3/5)
Release Date: 29.12.2019

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.

Description

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.

Vendor

WEMS Limited - https://www.wems.co.uk

Affected Version

2.58.8903
2.55.8806
2.55.8782
2.19.7959

Tested On

Linux
PHP

Vendor Status

[06.07.2019] Vulnerability discovered.
[13.08.2019] Vendor contacted.
[29.08.2019] No response from the vendor.
[30.08.2019] Vendor contacted.
[02.09.2019] No response from the vendor.
[03.09.2019] Vendor contacted.
[28.12.2019] No response from the vendor.
[29.12.2019] Public security advisory released.

PoC

wems_emxss.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://exchange.xforce.ibmcloud.com/vulnerabilities/173666
[2] https://cxsecurity.com/issue/WLB-2020010032
[3] https://packetstormsecurity.com/files/155777
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-21993
[5] https://nvd.nist.gov/vuln/detail/CVE-2020-21993

Changelog

[29.12.2019] - Initial release
[24.01.2020] - Added reference [1], [2] and [3]
[19.06.2021] - Added reference [4] and [5]

Contact

Zero Science Lab

Web: http://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Profiles**

-