ETAP Safety Manager 1.0.0.32 Remote Unauthenticated Reflected XSS

Title: ETAP Safety Manager 1.0.0.32 Remote Unauthenticated Reflected XSS
Advisory ID: ZSL-2022-5711
Type: Local/Remote
Impact: Cross-Site Scripting
Risk: (4/5)
Release Date: 11.09.2022

Summary

The ETAP Safety Manager (ESM) is a central managing and control system that helps you to monitor, adjust and maintain your emergency lighting system. Therefore each luminaire connected to your ESM network is given a unique code. The ESM can easily identify the luminaires individually and automatically report whether all luminaires work properly. You can either choose between a wired or wireless network, or a combination of both. With ESM you will not only manage your self contained or your centrally supplied 'ETAP Battery System' (EBS) emergency luminaires', but also DALI emergency units and K9 LED modules, which you can build into your luminaires. Since your ESM system is connected to the Internet, you will always have access to it through the World Wide Web. ESMweb™ is an 'embedded web server' application for monitoring an emergency lighting system, which runs in the 'ESM web controller'. The ESMweb™ application can be accessed from any PC in the corporate network or connected to the Internet - by a standard web browser.

Description

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

Vendor

ETAP Lighting International NV - https://www.etaplighting.com

Affected Version

1.0.0.32

Tested On

Apache/2.4.41 (Ubuntu)

Vendor Status

N/A

PoC

etap_xss.txt

Credits

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

References

[1] https://packetstormsecurity.com/files/168339/
[2] https://exchange.xforce.ibmcloud.com/vulnerabilities/235743
[3] https://cxsecurity.com/issue/WLB-2022090031

Changelog

[11.09.2022] - Initial release
[12.09.2022] - Added reference [1]
[13.09.2022] - Added reference [2]
[14.09.2022] - Added reference [3]

Contact

Zero Science Lab

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

- **Rete mirabilia**
- **We Suggest**

- **Profiles**

- Site Meter