Delta Controls enteliTOUCH 3.40.3935 Cross-Site Request Forgery (CSRF)

Title: Delta Controls enteliTOUCH 3.40.3935 Cross-Site Request Forgery (CSRF)
Advisory ID: ZSL-2022-5702
Type: Local/Remote
Impact: Cross-Site Scripting
Risk: (3/5)
Release Date: 14.04.2022

Summary

enteliTOUCH - Touchscreen Building Controller. Get instant access to the heart of your BAS. The enteliTOUCH has a 7-inch, high-resolution display that serves as an interface to your building. Use it as your primary interface for smaller facilities or as an on-the-spot access point for larger systems. The intuitive, easy-to-navigate interface gives instant access to manage your BAS.

Description

The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Vendor

Delta Controls Inc. - https://www.deltacontrols.com

Affected Version

3.40.3935
3.40.3706

3.33.4005

Tested On

DELTA enteliTOUCH

Vendor Status

[06.04.2022] Vulnerability discovered.
[06.04.2022] Vendor contacted.
[13.04.2022] No response from the vendor.
[14.04.2022] Public security advisory released.

PoC

entelitouch_csrf.html

Credits

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

References

[1] https://www.exploit-db.com/exploits/50878
[2] https://packetstormsecurity.com/files/166727/
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/224337
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29735
[5] https://nvd.nist.gov/vuln/detail/CVE-2022-29735

Changelog

[14.04.2022] - Initial release
[20.04.2022] - Added reference [1], [2] and [3]
[29.05.2022] - Added reference [4] and [5]

Contact

Zero Science Lab

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

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

- **Profiles**

- Site Meter