Halo Home Smart Lighting Vulnerability Advisory Communication CVE-2019-5625

Date:	14.05.2019
Subject:	Halo Home Smart Lighting Vulnerability Advisory
Severity rating:	Medium (5.3)
Product:	Halo Home Smart Lighting Mobile App
Affected version:	1.9.0

Summary

Eaton was recently contacted by Rapid 7 regarding the vulnerabilities that were discovered in Halo Home smart lighting mobile app and the Web based APIs used by the Mobile app (V 1.9.0). (Insecure data storage and Insecure direct object reference) (CVE-2019-5625)

By exploiting these vulnerabilities, attackers can impersonate as legitimate users and can learn private information like email address, on/off status of lighting systems etc. about potential targets.

Recommended Course of action

A new version of the Mobile app has been released that remediates these vulnerabilities.

Eaton recommends all the customers using Halo Home smart lighting mobile app to upgrade to the new version. Please download the latest Mobile App (1.11.0 or later) from Google Play Store and Apple App store.

Support

For additional information or a list of vulnerabilities that have been reported on our products and how to address them please visit our Cybersecurity web site www.eaton.com/cybersecurity or you can contact us at CybersecurityCOE@eaton.com.

Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in XXX
Publication No. BRXXXXXXXXE / XXX
July 2017

Follow us on social media to get the latest product and support information.