tyco

PRODUCT SECURITY ADVISORY

4–September–2018 CPP-PSA-2018-02 v1

Software House: IP-ACM v1

CVE-2017-17704

[This information was originally published in the Technical Advisory Bulletin SWH-TAB-000023234 dated January 11, 2018. The content has been updated and expanded.]

On December 18, 2017 security researchers from Google disclosed a vulnerability in the Software House product IP-ACM v1. This vulnerability was added to the National Vulnerability Database as CVE-2017-17704 on December 30th, 2017.

Details

The IP-ACM is a network door controller which provides physical access control capabilities including communication with card readers and door lock control. While it can operate independently in cases of network failure, the IP-ACM communicates to an iSTAR Ultra GCM to receive updates to the access control database and respond to user actions like manual door unlock.

The communications between the IP-ACM and the iSTAR Ultra GCM is encrypted with AES 256. However, the IP-ACM v1 uses a fixed key and initialization vector allowing an attacker with knowledge of this key and local network access the ability to decrypt the communication between the IP-ACM and iSTAR Ultra GCM. The encryption is also the only source of authentication for the IP-ACM v1, so an attacker who has compromised this vulnerability can replay commands sent from the iSTAR Ultra GCM to the IP-ACM.

Mitigation:

The hardware capabilities of the initial IP-ACM v1 product does not allow for an update to the firmware to address this issue. Shortly after the initial launch, an updated hardware platform was designed with additional processing and memory to support TLS communication. This second generation of the IP-ACM (IP-ACM v2) hardware and firmware are not susceptible to this vulnerability.

For customers with first generation hardware (see table below), the IP-ACM should be located on an isolated VLAN or physical network. The iSTAR Ultra GCM allows IP-ACM

Johnson Controls

communication through the second network interface port isolating the iSTAR Ultra GCM and IP-ACM traffic from the rest of the iSTAR network.

Note:

The original disclosure identifies the iSTAR Ultra as an affected product. While the exploit is on the communication between the iSTAR Ultra GCM and IP-ACM, the vulnerability exists only in the first generation of the IP-ACM firmware. The iSTAR Ultra GCM itself is not impacted by this vulnerability beyond its communication to the original IP-ACM hardware.

The affected units were sold starting in May 2016. The IP-ACM v2 replacement (see table below) became available in February 2018. The first generation of the IP-ACM has been discontinued from manufacturing.

Affected Models

Model Numbers	Description
IP-ACM2-MB	IP-ACM v1, board only
IP-ACM2-EM	IP-ACM v1 in metal enclosure
IP-ACM2-EP	IP-ACM v1 in plastic enclosure

Unaffected Models

Model Numbers	Description
IP-ACM2A-MB	IP-ACM v2, board only
IP-ACM2A-EM	IP-ACM v2 in metal enclosure
IP-ACM2A-EP	IP-ACM v2 in plastic enclosure

References

National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2017-17704

Disclosure: https://systemoverlord.com/2017/12/18/cve-2017-17704-broken-cryptography-in-istar-ultra-ip-acm-by-software-house.html

Please visit the Tyco security solutions, Cyber Protection website to register for and download security advisories.

Sincerely,
Product Security Team