Important notice for JACE 8000 and JACE 700 users

Current hardware could be impacted by Wi-Fi WPA/2 protocol vulnerabilities

Dear valued OEM partner,

This is an important notice for users of the JACE 8000 and JACE 700 regarding Wi-Fi Protected Access II (WPA2).

ISSUE
On Monday, October 16, the United States Computer Emergency Readiness Team (US-CERT) published Vulnerability Note VU #228519 regarding a Wi-Fi Protected Access II (WPA2) vulnerability:

"Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a wireless access point (AP) or client. An attacker within range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocols being used. Attacks may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast and group-addressed frames."

This means that Wi-Fi transmissions could be intercepted, and an attacker exploiting this vulnerability might be able to see transmitted information from devices using Wi-Fi, or even replay commands to or from devices on the Wi-Fi network, unless you have other security mechanisms that would mitigate this vulnerability.

IMPACTED TRIDIUM PRODUCTS
The following products incorporate Wi-Fi technology, and could be impacted by recently released Wi-Fi WPA/2 protocol vulnerabilities:

- JACE 8000
- JACE 700 using T7-WIFI Option Module

To date, no issues associated with this vulnerability have been reported to Tridium.

CUSTOMER ACTIONS

Tridium takes the security of our products seriously, and we are actively assessing the impact of these findings on our products and identifying corrective actions. We will be communicating with our customers on how best to mitigate and fix any vulnerabilities.

In the interim, the remedy for both the JACE 8000 users who enable Wi-Fi and all JACE 700 users who purchased the Wi-Fi Option card is the same. To mitigate risk:

- **If Wi-Fi is not needed,** users should disable it completely.
- **If Wi-Fi is needed,** users should ensure configuration is set to enable only encrypted communication for FOXS and HTTPS for both platform and station access. Please note: The default configuration for the JACE 8000 includes disabled Wi-Fi and encrypted communications.

FOR MORE INFORMATION

As we work to develop a long-term solution, please feel free to contact your Tridium account manager directly, or email our Tech Support team at support@tridium.com with questions.

We will provide updates as they are available.