AirLink Raven Security Vulnerability 10-January, 2014

Introduction

On 7-Jan 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the US Department of Homeland Security issued an advisory (ICSA-14-007-01) highlighting security vulnerabilities in the Raven X EV-DO. The purpose of this notice is to give further technical background on these vulnerabilities and offer approriate mitigation strategies.

Technical Background

The vulnerabilities addressed in the advisory relate to the device's firmware update mechanism. During the update process, password data is transmitted to the device. If a malicious entity were able to capture data packets transmitted during the firmware update process, they could use the captured data to reprogram the device at a later time.

Recommended Mitigation

Sierra Wireless recommends the following steps to mitigate this vulnerability:

- Do not perform firmware updates over the LAN or over the air. If device firmware needs to be updated, this should be done by directly attaching a PC running the firmware update tool to the device via an Ethernet cable. We are investigating methods to perform secure firmware updates remotely, and will provide information on this method when available.
- Disable over-the-air programming of the device. See the ALEOS 4.0.11 Configuration User Guide page 162 for details on how to disable over-the-air programming.
- Regular periodic updates to device passwords are recommended as a general network security practice. See the ALEOS 4.0.11 Configuration User Guide page 161 for details on how to change the device password.
- For high-security applications such as critical infrastructure monitoring, Sierra Wireless advises customers to deploy cellular devices using a Private Cellular Network or VPN to reduce the risk of an attacker capturing data transferred to/from the device.

Affected Products

Products affected by this vulnerability include the Raven X, Raven XE, Raven XT, PinPoint X, PinPoint XT and MP Products.

The GX400, GX440 and LS300 use a different firmware update mechanism that is not vulnerable to this issue.

Further Information

For further inquiries, please contact support@sierrawireless.com or visit our support website for any updates to this notice.