Sierra Wireless Technical Bulletin:
ICS-ALERT-16-182-01 / CCIRC AL16-014

Products: Sierra Wireless Raven XE and XT gateways

Date of issue: 25 April 2017

Sierra Wireless has received a report of security issues affecting the Raven XE and XT gateway products. These issues are covered by advisories from ICS-CERT and CCIRC:

- ICS-CERT: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-16-182-01
- CCIRC: http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2016/al16-014-en.aspx

This bulletin provides an overview of the identified issues along with recommended mitigation actions.

Issues identified

Issue identified by ICS-CERT	Sierra Wireless Response	Recommended Actions
CVE-2017-6042: Cross-site request forgery	This issue may allow an attacker to execute unauthorized operations on the gateway by convincing an authorized user who has logged into the gateway to click on a malicious link. This issue has been addressed in ALEOS 4.0.14.	Upgrade to ALEOS 4.0.14. In the interim, customers are advised to avoid clicking on externally provided links while logged into ACEmanager and to log out of ACEmanager when access to configuration and status is no longer required (2).
CVE-2017-6046: Vulnerable to credential sniffing	This issue may affect users who are connecting to the gateway over an insecure network. For example, a public Wi-Fi hotspot or a compromised corporate network.	Do not access ACEmanager over unsecured networks (3). Where possible, directly connect to the gateway when accessing ACEmanager (4).

CVE-2017-6044: Unauthenticated access/Arbitrary file upload	This issue may allow an attacker to steal user credentials or execute unauthorized actions when an authorized user logs in to ACEmanager. This issue has been addressed in ALEOS 4.0.14.	Upgrade to ALEOS 4.0.14. In the interim, disable remote access to ACEmanager and ensure that local USB and Ethernet interfaces on the gateway are physically secured (1).

Products covered by this bulletin

This bulletin applies to all Sierra Wireless Raven XE and XT gateways.

Summary of Recommended Actions

In order to safeguard against potential impacts due to these issues, Sierra Wireless recommends performing the following actions:

1. Upgrade to ALEOS 4.0.14. Prior to availability and deployment of the new software, Sierra Wireless advises disabling remote access to ACEmanager and ensuring that local USB and Ethernet interfaces on the gateway are physically secured. Remote access to ACEmanager can be disabled as follows:
    a. Log in to ACEmanager and navigate to *Services > ACEmanager*
    b. Set *OTA ACEmanager Access* to *OFF*
    c. Click *Apply* then reboot the gateway.
2. Avoid clicking on externally provided links while logged into ACEmanager and log out of ACEmanager when access to configuration and status is no longer required.
3. Do not access ACEmanager over unsecured networks.
4. Where possible, directly connect to the gateway when accessing ACEmanager.

Further Information

For further information and technical support, please contact your authorized AirLink reseller or Sierra Wireless representative. For information on how to contact Sierra Wireless, please visit https://www.sierrawireless.com/company/contact-us/