Multiple Vulnerabilities in Sierra Wireless Routers

Severity Level: High

Components Affected

- Sierra Wireless AirLink cellular routers
- TinyXML
- OpenNDS.

Overview

A collection of 21 vulnerabilities have been discovered in Sierra Wireless AirLink cellular routers and open-source software components like TinyXML and OpenNDS.

Description

The vulnerabilities are in Sierra Wireless AirLink routers and stem from various open source components used in the routers, like an open source captive portal called OpenNDS and an open source XML document parser called TinyXML, which is also an abandoned project. If exploited, the bugs can have several potential impacts, from allowing attackers to steal credentials to enabling them to take control of routers via code injection. Among the 21 vulnerabilities, one has critical severity (CVSS score 9.6), nine have high severity, and 11 have medium severity.

Impact

- Remote code execution (RCE)
- Cross-site scripting (XSS)
- Denial-of-service (DoS)
- Unauthorized access
- Authentication bypasses
- Adversary-in-the-middle (AitM) attacks

Solution/ Workarounds

Sierra Wireless has released the following ALEOS versions to address the new vulnerabilities:

- ALEOS 4.17.0 containing fixes for all relevant vulnerabilities.
- ALEOS 4.9.9 containing applicable fixes, except for OpeNDS issues since that version does not include OpenNDS.

Further, it is recommended to take the following additional actions for enhanced protection:

- Change default SSL certificates in Sierra Wireless routers and similar devices.
- Disable or restrict non-essential services like captive portals, Telnet, and SSH.
- Implement a web application firewall to protect OT/IoT routers from web vulnerabilities.
- Install an OT/IoT-aware IDS to monitor external and internal network traffic for security breaches.

Reference

- https://thehackernews.com/2023/12/sierra21-flaws-in-sierra-wireless.html
- https://www.bleepingcomputer.com/news/security/sierra-21-vulnerabilities-impact-critical-infrastructure-routers/

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.