Product Security Advisory: ALEOS Security Advisory

Sierra Wireless Advisory: SWI-PSA-2023-006 R4

Release History

Revision	Date	Notes
R4	14 December 2023	Revised with additional detail relating to recommended actions for the RV50
R3	11 December 2023	Revised with additional detail on the impact of specific mitigation as well as clarifying language.
R2	07 December 2023	Revised to include additional vulnerabilities in OpenNDS with guidance on their impact on ALEOS.
R1	28 November 2023	Initial Release

Summary

Sierra Wireless was recently informed of eight security vulnerabilities in ALEOS, the operating system used in certain Sierra Wireless AirLink Routers, including the MP70, RV50X, RV55, LX40, LX60 ES450 and GX450. Sierra Wireless was also informed of fourteen vulnerabilities affecting OpenNDS, an open-source component used in ALEOS to provide simple captive portal functionality, eight of which affect ALEOS in the configuration supplied by Sierra Wireless. The vulnerabilities are present in ALEOS 4.16 and earlier versions and have been remediated in ALEOS 4.17 released in October 2023.

CVE ID	Description	CVSSv3.1
CVE-2023-40458	The ACEManager component of ALEOS 4.16 and earlier uses an open-source component which is vulnerable to an infinite loop condition, which could potentially allow a remote attacker to trigger a Denial of Service (DoS) condition for ACEManager without impairing	7.5

	other router functions. This condition is cleared by restarting the router.	
CVE-2023-40459	The ACEManager component of ALEOS 4.16 and earlier does not adequately perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5
CVE-2023-40460	The ACEManager component of ALEOS 4.16 and earlier does not validate uploaded file names and types, which could potentially allow an authenticated user to perform client-side script execution within ACEManager, altering the router functionality until the router is restarted.	7.1
CVE-2023-40461	The ACEManager component of ALEOS 4.16 and earlier allows an authenticated user with Administrator privileges to access a file upload field which does not fully validate the file name, creating a Stored Cross-Site Scripting condition.	8.1
CVE-2023-40462	The ACEManager component of ALEOS 4.16 and earlier does not perform input sanitization during authentication, which could potentially result in a Denial of Service (DoS) condition for ACEManager without impairing other router functions. ACEManager recovers from the DoS condition by restarting within ten seconds of becoming unavailable.	7.5
CVE-2023-40463	When configured in debugging mode by an authenticated user with administrative privileges, ALEOS 4.16 and earlier store the SHA512	8.1

	hash of the common root password for that version in a directory accessible to a user with root privileges or equivalent access.	
CVE-2023-40464	Several versions of ALEOS, including ALEOS 4.16.0, use a hardcoded SSL certificate and private key. An attacker with access to these items could potentially perform a man in the middle attack between the ACEManager client and ACEManager server.	8.1
CVE-2023-40465	Several versions of ALEOS, including ALEOS 4.16.0, include an open-source third-party component which can be exploited from the local area network, resulting in a Denial of Service condition for the captive portal. This vulnerability could potentially be exploited to trigger Remote Code Execution in the root context.	DoS 4.3 RCE 8.3

OpenNDS Vulnerabilities

The vulnerabilities noted below were disclosed by OpenNDS, an open-source component used within ALEOS. While many of these vulnerabilities are not applicable to ALEOS in the configuration used by Sierra Wireless, remediations were introduced in the ALEOS 4.17.0.12 release. OpenNDS is not used by ALEOS 4.9.x.

The vulnerabilities in OpenNDS noted in this Security Bulletin are not exploitable if the 'Simple Captive Portal' is not enabled in ALEOS.

Note: RV50 routers, while no longer supported, do not include Wi-Fi functionality and therefore are not impacted by the OpenNDS vulnerabilities.

CVE ID	Description	CVSSv3.1
CVE-2023-38313	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered with a crafted GET request to /opennds_auth/ with a missing client-redirect query string parameter and client-token and custom query string parameters set to arbitrary values. The issue occurs when a client is about to be authenticated and takes place via a different code path than CVE-2023-38314. Triggering the issue crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5
CVE-2023-38314	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered with a crafted GET request to /opennds_auth/ with a missing client-redirect query string parameter and a client-token query string parameter set to an arbitrary value. The issue occurs while a client is not yet authenticated. Triggering the issue crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5
CVE-2023-38315	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered with a crafted GET request to /opennds_auth/ with a missing client-token query string parameter. Triggering the issue crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5

CVE-2023-38320	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered via a crafted GET request to /opennds_auth/ with a missing custom query string parameter and client-token and redirect query string parameters set to arbitrary values. Triggering the issue 6.5 DoS TRUE Sierra:21 – Living on the Edge 9 crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5
CVE-2023-38321	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered via a crafted GET request to /opennds_auth/ with a missing custom query string parameter and client-token and redirect query string parameters set to arbitrary values. Triggering the issue 6.5 DoS TRUE Sierra:21 – Living on the Edge 9 crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5
CVE-2023-38322	OpenNDS has a NULL-pointer dereference that leads to a DoS. The issue can be triggered via a crafted GET request to /opennds_auth/ with a missing User-Agent header and client-token, custom, and redirect query string parameters set to arbitrary values. The issue occurs when a client is about to be authenticated and happens via a different code path than CVE-2023-38320. Triggering the issue crashes the OpenNDS daemon and denies Internet access to any client that attempts to connect with this captive portal. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	6.5

CVE-2023-38316	When the custom URL unescape callback is enabled in OpenNDS, unauthenticated attackers can execute arbitrary OS commands by inserting them into the URL portion of the GET request. **This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.**	8.8
CVE-2023-38317	OpenNDS does not sanitize the network interface name entry in the configuration file, allowing attackers that have direct or indirect access to the file to execute arbitrary OS commands. **This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.**	6.7
CVE-2023-38318	OpenNDS does not sanitize the gateway FQDN entry in the configuration file, allowing attackers that have direct or indirect access to the file to execute arbitrary OS commands. **This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.**	6.7
CVE-2023-38319	OpenNDS does not sanitize the FAS key entry in the configuration file, allowing attackers that have direct or indirect access to the file to execute arbitrary OS commands. **This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.**	6.7
CVE-2023-38323	OpenNDS does not sanitize the status path script entry in the configuration file, allowing attackers that have direct or indirect access to the file to execute arbitrary OS commands.	6.7

	This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.	
CVE-2023-38324	When OpenNDS is configured as FAS, and the default FAS key is used, users can skip the splash page sequence and authenticate directly. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	4.3
CVE-2023-41101	OpenNDS (and the original NoDogSplash project) do not validate the length of the query string of pre-authenticated GET requests. This leads to a stack-based buffer overflow in NoDogSplash and OpenNDS versions 9.x and earlier, and to a heap-based buffer overflow in OpenNDS versions 10.x and onward. Attackers may exploit the issue for DoS or to execute arbitrary code. **This vulnerability affects ALEOS prior to release 4.17.0.12.**	9.6
CVE-2023-41102	OpenNDS (up to version 10.1.2) has multiple memory leaks due to not freeing up allocated memory. This may lead to a DoS due to the consumption of all available memory. **This vulnerability is not exposed in the released ALEOS configuration of OpenNDS.**	4.3

Affected Products

These vulnerabilities, with the exception of OpenNDS vulnerabilities which do not affect ALEOS 4.9.x, affect all AirLink routers running ALEOS software releases prior to version 4.9.9 (ES450, GX450) and prior to 4.17.0.12 (MP70, RV50X, RV55, LX40, LX60).

Recommended Actions

For MP70, RV50X, RV55, LX40, LX60 routers

If your gateway is on ALEOS 4.16 upgrade to ALEOS 4.17.0.12 as soon as possible.

If your gateway is on a release earlier than ALEOS 4.16 upgrade to ALEOS 4.16, then to ALEOS 4.17.0.12 as soon as possible.

Pending upgrade we recommend following the mitigations described in the “Recommended Mitigation” section below.

For ES450, GX450 routers

If your gateway is on release ALEOS 4.9.X upgrade to ALEOS 4.9.9 as soon as possible.

Pending upgrade we recommend following the mitigations described in the “Recommended Mitigation” section below.

For RV50 and other routers that are no longer receiving security updates

For RV50 and other routers that are no longer receiving security updates we recommend refeshing these routers with actively supported routers. Pending the router refresh we recommend following the mitigations described in the “Recommended Mitigation” section below where applicable to reduce the risk associated with these potential vulnerabilities.

Recommended Mitigation

The following configuration change based mitigations are recommended:

1. Always use strong, and ideally unique random credentials for your routers.

2. Disable, if previously enabled, access to ACEManager on the WAN and make use of the Sierra Wireless Airlink Management System (ALMS) or an alternative router management platform for remote management of your ALEOS routers. Disabling access to ACEManager on the WAN will reduce the attack surface, limiting exploitation of vulnerabilities affecting ACEManager to the LAN and WLAN interfaces.

3. If you must leave ACEManager accessible via the WAN, restrict access using measures such as Private APN, VPN, or the ALEOS Trusted IP feature that restricts access to specific hosts.

4. Disable the diagnostic shell, if previously enabled, on AirLink routers when not being used for diagnostic purposes.

6. Disable, if previously enabled and not in use, 'Simple Captive Portal' on the router to prevent OpenNDS from launching. If 'Simple Captive Portal' is disabled, OpenNDS vulnerabilities will not be exploitable.

Credit

Sierra Wireless would like to thank Dr. Stanislav Dashevskyi of ForeScout for bringing these issues to our attention. We encourage anyone with a security concern related to Sierra Wireless products to please contact us at security@sierrawireless.com.

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll-Free): 1-877-687-7795
Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:
https://www.sierrawireless.com/company/security/