Product Security Advisory: Vulnerabilities in Dnsmasq

Sierra Wireless Advisory: SWI-PSA-2021-002 (link to latest version)

Date January 20, 2021

Summary

Recently published research has identified two sets of vulnerabilities in dnsmasq, one set of memory corruption issues handling DNSSEC and a second set of issues validating DNS responses. The following Common Vulnerability and Exposure (CVE) identifiers have been assigned to each of the vulnerabilities:

DNSSEC handling code.

- CVE-2020-25681 (CVSS 8.1) A heap-based buffer overflow in dnsmasq in the way it sorts RRSets before validating them with DNSSEC data.
- CVE-2020-25682 (CVSS 8.1) A buffer overflow vulnerability in the way dnsmasq extract names from DNS packets before validating them with DNSSEC data.
- CVE-2020-25683 (CVSS 5.9) A heap-based buffer overflow in get_rdata subroutine of dnsmasq, when DNSSEC is enabled and before it validates the received DNS entries.
- CVE-2020-25687 (CVSS 5.9) A heap-based buffer overflow in sort_rrset subroutine of dnsmasq, when DNSSEC is enabled and before it validates the received DNS entries.

DNS response validation.

- CVE-2020-25684 (CVSS 4.0) Dnsmasq does not validate the combination of address/port and the query-id fields of DNS request when accepting DNS responses.
- CVE-2020-25685 (CVSS 4.0) Dnsmasq uses a weak hashing algorithm (CRC32) when compiled without DNSSEC to validate DNS responses.
- CVE-2020-25686 (CVSS 4.0) Dnsmasq does not check for an existing pending request for the same name and forwards a new request thus allowing an attacker to do a "Birthday Attack" scenario to forge replies and potentially poison the DNS cache.

Affected Products

The following table lists the product impacts of the two sets of vulnerabilities listed above and the current state of remediation planning. This bulletin will be updated when firmware update release dates are finalized. Please visit https://sierrawireless.com/security for the latest information.

Product	DNSSEC Handling Code	DNS Response Validation	Fix Version	Target Release Date
ALEOS 4.4.X	Not Affected	Affected	No Fix Planned	No Fix Planned
ALEOS 4.9.x	Not Affected	Affected	4.9.6	February 2021
ALEOS 4.14.x	Not Affected	Affected	4.15.0	June 2021
Airlink OS 2.0	Not Affected	Affected	Airlink OS 2.1	June 2021
Airlink OS 20.06	Not Affected	Affected	Airlink OS 2.1	June 2021
ACM 2.1(FIPS)	Not Affected	Affected	ACM 2.1.1	October 2021
WP76xx	Affected	Affected	R17 BP7	April 2021
WP77xx	Affected	Affected	R15	TBD
WP85xx	Affected	Affected	No Fix Planned	No Fix Planned

Recommended Actions

Sierra Wireless recommends upgrading to the latest version for your products as soon as they become available.

Credits

Sierra Wireless would like to thank JSOF for discovering and responsibly reporting these issues, as well as the efforts of CERT/CC for coordinating the response. For more information please refer to the links below:

https://www.jsof-tech.com/disclosures/dnspooq/

https://kb.cert.org/vuls/id/434904

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/