

Silicon Labs Security Advisory

A-00000515

Subject: Azure NetX vulnerabilities impacting RS9116 and SiWx917 products

CVSS Severity: High

Base Score: 9.8, Critical

Temporal Score: 8.2, High

Vector String: [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:R](#)

Impacted Products

Product	Impacted Version
RS9116W	WiSeConnect v2.10.2, and earlier, delivered as part of SiSDK v2024.6.1 and earlier.
SiWx917	WiSeConect v3.3.2, and earlier, delivered as part of SiSDK v2024.6.1 and earlier.

Please note: As of June 2024, the Gecko SDK was renamed to the Simplicity SDK, and the versioning scheme was changed from Gecko SDK vX.Y.Z to Simplicity SDK YYYY.MM.Patch#.

CVE ID(s)

The following CVEs were published for these vulnerabilities:

- [CVE-2023-48315](#) [1]
- [CVE-2023-48316](#) [2]
- [CVE-2023-48691](#) [3]
- [CVE-2023-48692](#) [4]

Technical Summary

- 4 independent vulnerabilities in the Azure NetX TCP/IP stack, used by the wireless firmware on the RS9116 and SiWx917-based products may lead to remote code execution.

Fix/Workaround

- Impacted RS9116 customers should upgrade to WiSeConnect v2.10.3, or later, delivered as part of SiSDK v2024.6.2, and update the connectivity firmware on all devices. Instructions for updating can be found in [AN1290: RS9116W Firmware Update Application Note](#).
- Impacted SiWx917 customers should upgrade to WiseConnect v3.3.3, or later, delivered as part of SiSDK v2024.6.2 and update the connectivity firmware on all devices. Instructions for updating the connectivity firmware for SoC devices are found [here](#)[8]. Instructions for updating the connectivity firmware for NCP devices are found [here](#)[9].
- Instructions for [downloading/updating the SiSDK](#) [6] and for [upgrading a project to use a new SiSDK version](#) [7] can be found in the Simplicity Studio Users Guide.

References

- [1] <https://nvd.nist.gov/vuln/detail/CVE-2023-48315>
- [2] <https://nvd.nist.gov/vuln/detail/CVE-2023-48316>
- [3] <https://nvd.nist.gov/vuln/detail/CVE-2023-48691>
- [4] <https://nvd.nist.gov/vuln/detail/CVE-2023-48692>
- [5] <https://www.silabs.com/documents/login/application-notes/an1290-rs9116w-firmware-update-application-note.pdf>
- [6] <https://docs.silabs.com/simplicity-studio-5-users-guide/latest/ss-5-users-guide-about-the-launcher/toolbar#install>
- [7] <https://docs.silabs.com/simplicity-studio-5-users-guide/latest/ss-5-users-guide-getting-started/project-upgrade-new-gsdk-version>
- [8] <https://docs.silabs.com/wiseconnect/3.3.0/wiseconnect-developers-guide-developing-for-silabs-hosts/#update-si-wx91x-connectivity-firmware>
- [9] <https://docs.silabs.com/wiseconnect/3.3.0/wiseconnect-getting-started/getting-started-with-ncp-mode-with-efr32#update-si-wx91x-connectivity-firmware>

Revision History

Rev	Date	Description of Changes
1.0	2024-OCT-10	Initial publication

Guidelines on our security vulnerability policy can be found at <https://www.silabs.com/security>
For Silicon Labs Technical Support visit: <https://www.silabs.com/support>

Notice: The contents of this Notification are provided exclusively for the internal use of the recipient in support of devices supplied by Silicon Labs and shall not be shared with or distributed to any third parties. This Notification shall not be posted on any blog, website, board or social media. The contents are for general information only and do not purport to be comprehensive. While Silicon Labs provides this information in good faith and makes every effort to supply correct, current and high-quality guidance, Silicon Labs provides all materials (including this document) solely on an "as is" basis without warranty of any kind. Silicon Labs disclaims all express and implied warranties. In no event shall Silicon Labs be liable for any damages whatsoever, including direct, indirect, incidental, consequential, lost profits or special damages related to or arising from the adequacy, accuracy, completeness or timeliness of this document or its contents, even if Silicon Labs has been advised of the possibility of such damages. Nothing in this Notice excludes any liability for death or personal injury caused by negligence, or for fraud or intentional misrepresentation. By accepting or using the information contained in this Notification, the recipient agrees to that this Notification and its use are governed by the laws of the State of Texas, excluding its conflicts of law's provisions.