Silicon Labs Security Advisory

A-00000526

Subject: DLL hijacking vulnerabilities present in Silicon Labs tooling installers

CVSS Severity: High

Base Score: 8.6, High
Temporal Score: 8.1, High
Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:F/RL:X/RC:R

Note: Starting December 1, 2024, Silicon Labs PSIRT will use CVSS 4.0 to measure the impact of newly reported vulnerabilities.

Impacted Products

- The products listed in the following table are impacted by these vulnerabilities.

Product	Description	Impacted Version
Silicon Labs IDE	8051 MCU Software	All released versions (v5.50 and earlier)
Configuration Wizard 2	8051 MCU Software	All released versions (v4.50 and earlier)
Flash Programming Utility	8051 MCU Software	All released versions (v4.80 and earlier)
ToolStick	8051 MCU Software	All released versions (v2.60.1 and earlier)
CP210 VCP Win 2k Drivers	USB to UART Bridge VCP Drivers	v6.3 and earlier
CP210x VCP Windows Drivers	USB to UART Bridge VCP Drivers	v6.7 and earlier
USBXpress Dev Kit	Interface Direct Access Drivers	v3.5.1 and earlier
USBXpress 4 SDK	Interface Direct Access Drivers	v4.0.3 and earlier
USBXpress SDK	Interface Direct Access Drivers	v6.7.4 and earlier
USBXpress Win 98SE Dev Kit	Interface Direct Access Drivers	v2.42 and earlier

CVE IDs

- The CVEs listed in the following table are reserved for these vulnerabilities.

CVE Number	Description
CVE-2024-9490	Uncontrolled search path can lead to DLL hijacking in Silicon Labs IDE installer
CVE-2024-9491	Uncontrolled search path can lead to DLL hijacking in Configuration Wizard 2 installer
CVE-2024-9492	Uncontrolled search path can lead to DLL hijacking in Flash Programming Utility installer
CVE-2024-9493	Uncontrolled search path can lead to DLL hijacking in ToolStick installer
CVE-2024-9494	Uncontrolled search path can lead to DLL hijacking in CP210 VCP Win 2k installer
CVE-2024-9495	Uncontrolled search path can lead to DLL hijacking in CP210x VCP Windows installer
CVE-2024-9496	Uncontrolled search path can lead to DLL hijacking in USBXpress Dev Kit installer
CVE-2024-9497	Uncontrolled search path can lead to DLL hijacking in USBXpress 4 SDK installer
CVE-2024-9498	Uncontrolled search path can lead to DLL hijacking in USBXpress SDK installer
CVE-2024-9499	Uncontrolled search path can lead to DLL hijacking in USBXpress Win 98SE Dev Kit installer

Technical Summary

- DLL hijacking vulnerabilities, caused by an uncontrolled search path, present in Silicon Labs' installers can lead to privilege escalation and arbitrary code execution.
    - Exploit is only possible when running the impacted installer.

Fix/Workaround

- No fix is available for these issues. However, following the guidelines listed below may mitigate risks.
    - Always download Silicon Labs' installers directly from www.silabs.com.
    - Always download, install, and execute installers from a directory with limited write access.

Attribution

- CVE-2024-9490, CVE-2024-9491, CVE-2024-9492, CVE-2024-9493, CVE-2024-9496, CVE-2024-9497, CVE-2024-9498, and CVE-2024-9499 were discovered by security researchers Sahil Shah and Shaurya.

- CVE-2024-9494 was discovered by security researchers Sahil Shah, Shaurya, and Ramya Shah.
- CVE-2024-9495 was discovered by security researchers Sahil Shah, Shaurya, and Vidhi Patel.

Revision History

Rev	Date	Description of Changes
1.1	2025-JAN-27	Updated attribution section
1.0	2025-JAN-23	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