Bluetooth Keystroke-Injection Flaw: A Threat To Apple, Linux & Android Devices

December 7, 2023 By **Guru Baran**

An unauthenticated Bluetooth keystroke-injection vulnerability that affects Android, macOS, and iOS devices has been discovered.

This vulnerability can be exploited by tricking the Bluetooth host state machine into pairing with a fake keyboard without authentication.

This vulnerability affects Android devices with Bluetooth enabled, Linux/BlueZ devices with Bluetooth Connectable/Discoverable iOS and macOS with Bluetooth enabled, and Magic Keyboard paired with the phone or computer.

The CVE for this vulnerability has been assigned as CVE-2023-45866.

CVE-2023-45866: Unauthenticated Bluetooth Keystroke-Injection

After pairing with the target phone or computer, a threat actor can exploit this vulnerability from a Linux computer that uses a Standard Bluetooth adapter.

Once paired, the threat actor can inject keystrokes and perform arbitrary actions in the name of the victim, which does not require any authentication.

Affected Devices

Additionally, this vulnerability was successfully reproduced on the devices below.

- Pixel 7 running Android 14
- Pixel 6 running Android 13
- Pixel 4a (5G) running Android 13
- Pixel 2 running Android 11
- Pixel 2 running Android 10
- Nexus 5 running Android 6.0.1
- BLU DASH 3.5 running Android 4.2.2
- Ubuntu 18.04, 20.04, 22.04, 23.10
- 2022 MacBook Pro with MacOS 13.3.3 (M2)
- 2017 MacBook Air with macOS 12.6.7 (Intel)
- iPhone SE running iOS 16.6

ChromeOS was not found to be vulnerable to this attack as it was patched perfectly by Google.

The security researcher has not published a fully detailed report about this vulnerability. However, a GitHub repository that explains the impact and details of this vulnerability has been published.

The Linux vulnerability (CVE-2020-0556) has been fixed, but it seems like the fix was left disabled by default, which makes the devices still vulnerable to this attack vector.

BluZ has fixed this vulnerability and enabled the fix by default as of the fix of 2020.

Google will fix the vulnerabilities in currently supported Pixel devices via December OTA updates.