Bleeding Tooth

CVSS: 8.3

Background

The three vulnerabilities associated with BleedingTooth can be found in CVE-2020- 12351, CVE-2020-12352, and CVE-2020-24490. Each of these vulnerabilities affects BlueZ, the official Linux Bluetooth protocol stack. The most severe is CVE-2020-12351 with a CVSS of 8.3, a remote Bluetooth attack which when properly executed could allow an attacker to execute arbitrary code on the target device with kernel privileges.

The vulnerability described in CVE-2020-12351 can be exploited by a remote attacker within Bluetooth range of the target, and which knows the Bluetooth Address (BD_ADDR) of the target device. To trigger the flaw, the attacker sends a malicious L2cap packet, which can lead to denial of service or even execution of arbitrary code, with kernel privileges. An attacker looking to trigger the vulnerability can also use a malicious Bluetooth chip. Proof-of-concept code for an exploit can be found on GitHub. The bug is a zero-click vulnerability, in that it does not require user interaction to be exploited.

The second issue, CVE-2020-12352, is a stack-based information leak that impacts Linux kernel 3.6 and higher. The bug is considered medium severity with a CVSS score of 5.3. A remote attacker in close proximity to the target and knowing the victim's BD_ADDR can retrieve kernel stack information containing various pointers that can be used to predict the memory layout and to defeat kernel address space layout randomization (KASLR). The leak has the potential to contain other valuable information such as encryption keys.

Recorded in CVE-2020-24490 and also considered medium risk, the third vulnerability is a heapbased buffer overflow that affects Linux kernel 4.19 and higher. A remote attacker within short range of a vulnerable device can trigger the flaw through broadcasting extended advertising data. This could lead to denial of service or even arbitrary code execution with kernel privileges.

Any medical device that employs the Linux Bluetooth protocol stack BlueZ version 5.9 over lower is affected. Clinical systems and patient-wearable devices employing this stack should take immediate corrective measures, including updating to Linux kernel 5.9 or higher.