AL2022_260 New KCodes NetUSB Bug Affect Millions of Routers from Different Vendors (13th January 2022)

Description

Security experts revealed a potential critical weakness in the KCodes NetUSB module that has affected several million end-user routers ranging from Netgear, TP-Link, Tenda, EDiMAX, D-Link and Western Digital.

Summary

KCodes NetUSB is known as a type of Linux Kernel component that allows peripherals to offer USB-based connections over IP. The drivers for the various peripheral devices are connected to a Linux-based control platform that is available over the internet system.

According to a study shared by SentinelOne with The Hacker News, CVE-2021-45608 (CVSS score: 9.8) refers to a buffer overflow vulnerability weakness that, if attacked successfully, could allow attackers to execute commands remotely in the kernel and undertake malicious operations at one‘s desire.

How it works

Although this has been the most current line of NetUSB flaws which have been addressed in the past few years. SEC Consult researchers revealed a buffer overflow bug known as CVE-2015-3036 in May 2015, which could lead to a denial of service or carryout cypher attacks

In June 2019, another company known as Cisco Talos revealed information of two NetUSB flaws tracked as CVE-2019-5016 and CVE-2019-5017, which might allow a hacker to force Netgear wireless routers into divulging classified data and executing malware remotely.

Remediation

The following guidance below can help mitigate this vulnerability described in this alert:

• Check for firmware updates for your listed router and apply updates – Firmware updates helps to resolve software bug issues that can be vulnerabilities turned into exploits by attackers.

• Ensure your router has not reached the end of life (EOL) – once the router reaches EOL, routers will be exposed to any kind of vulnerability attacks. Applying a firewall at the perimeter of the network may help to mitigate attacks, but it is advised to replace the EOL router with a later model.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- New KCodes NetUSB bug affects millions of routers from different vendors (11th January 2022). Retrieved from thehackernews.

  https://thehackernews.com/2022/01/new-kcodes-netusb-bug-affect-millions.html

- New KCodes NetUSB bug affects millions of routers from different vendors (11th January 2022). Retrieved from Sentinel Labs.

  https://www.sentinelone.com/labs/cve-2021-45608-netusb-rce-flaw-in-millions-of-end-user-routers/