Microsoft expert discovered a series of serious code execution errors in IoT, OT devices

Microsoft security researchers announced that they discovered more than two dozen serious remote code execution (RCE) vulnerabilities related to Internet of Things (IoT) and Operational Technology (OT) devices being used. Relatively popular use today.

These 25 security flaws are collectively referred to as BadAlloc, and according to the initial investigation, they all stem from a glitch in the Integer Overflow or Wraparound memory allocation process. In theory, threat actors can exploit vulnerabilities to cause system crashes and even remotely execute malicious code on vulnerable IoT and OT systems. This is also the reason why they have a high severity rating.

Microsoft security team found these 25 BadAlloc vulnerabilities in a cluster of standard memory allocation functions widely used in many real-time operating systems (RTOS), standard deployment libraries. standard C (libc) and embedded software development kit (SDK).

> " Our research shows that many memory allocation implementations written over the years as part of IoT devices and embedded software have failed to incorporate input authentications. appropriate , "said a team representative from the Microsoft Security Response Center. " Without these input validations, an attacker could fully exploit the memory allocation function to perform a heap overflow, leading to remote execution of malicious code. on target device ".

BadAlloc vulnerable devices

The majority of IoT and OT devices that are susceptible to the aforementioned BadAlloc vulnerabilities are currently widely used in the consumer, medical and industrial networking sectors.

The complete list of devices affected by BadAlloc includes:

1. Amazon FreeRTOS, Version 10.4.1
2. Apache Nuttx OS, Version 9.1.0
3. ARM CMSIS-RTOS2, versions prior to 2.1.3
4. ARM Mbed OS, version 6.3.0
5. ARM mbed-uallaoc, Version 1.3.0
6. Cesanta Software Mongoose OS, v2.17.0
7. eCosCentric eCosPro RTOS, Versions 2.0.1 to 4.5.3
8. Google Cloud IoT Device SDK, Version 1.0.2
9. Linux Zephyr RTOS, versions prior to 2.4.0
10. Media Tek LinkIt SDK, previous versions 4.6.1
11. Micrium OS, Version 5.10.1 and earlier
12. Micrium uCOS II / uCOS III Version 1.39.0 and earlier
13. NXP MCUXpresso SDK, previous versions 2.8.2
14. NXP MQX, Version 5.1 and earlier
15. Redhat newlib, previous versions 4.0.0
16. RIOT OS, Version 2020.01.1
17. Samsung Tizen RT RTOS, previous version 3.0.GBB
18. TencentOS-tiny, Version 3.1.0
19. Texas Instruments CC32XX, previous versions 4.40.00.07
20. Texas Instruments SimpleLink MSP432E4XX
21. Texas Instruments SimpleLink-CC13XX, versions prior to 4.40.00
22. Texas Instruments SimpleLink-CC26XX, versions prior to 4.40.00
23. Texas Instruments SimpleLink-CC32XX, versions prior to 4.10.03
24. Uclibc-NG, previous versions 1.0.36
25. Windriver VxWorks, before 7.0

To minimize risk, organizations using a BadAlloc vulnerable device should:

1. Apply carrier updates available.
2. Minimize the network exposure of all devices or control systems, and ensure that they are not accessible from the Internet.
3. Locate the control system network and remote devices behind the firewall, and isolate them from the corporate network.
4. When remote access is required, use secure methods, such as virtual private network (VPN).

If vulnerable devices cannot be patched immediately, Microsoft recommends:

1. Narrow the attack surface by minimizing or eliminating the vulnerable devices' exposure to the internet;
2. Perform network security monitoring to detect indicators of intrusion;
3. Strengthen network segmentation to protect important data.