UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00147

25 CRITICAL IOT DEVICE VULNERABILITIES

DATE ISSUED: 24th May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Microsoft researchers Section 52 – Azure Defender for IoT group, are warning of 25 critical memory-allocation vulnerabilities across a range of vendor Internet of Things (IoT) or smart and industrial devices that are as yet undocumented and are collectively known as BadAlloc.

BREAKDOWN

It has been discovered that IoT devices over numerous years incorporate ineffective memory allocation implementations that do not include proper input validation. This could lead to memory attacks including heap overflow, which has the potential to allow malicious code execution. The use of vulnerable memory functions such as malloc, calloc, realloc, memalign, valloc, pvalloc and many more which are responsible for appropriately allocating memory for a device create significant and varied risk for any organisation these devices are present in and connected to the corporate network. This systemic problem can exist across numerous device aspects such as Real Time Operating Systems (RTOS), embedded Software Development Kits (SDKs), and C standard library (libc) implementations. Devices affected include Texas Instruments, ARM, Amazon and Samsung and many more. As yet, none of these vulnerabilities are seen to be exploited in the wild and vendors have been notified to take remediation and patching action for their devices where possible.

REMEDIATION STEPS

- See list of devices and remediation actions in sources below.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/microsoft-warns-25-critical-iot-industrial-devices/165752/
US CERT https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04