U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00190

REALTEK CHIPSETS SDK UNDER ACTIVE EXPLOIT

DATE ISSUED: 30th August 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

65 vendors are currently under active command-injection style attack due to numerous vulnerabilities discovered in the Realtek Software Developer Kits (SDKs) with one instance reporting attempts to install Mirai malware.

BREAKDOWN

It is noted that attackers appear to be actively hunting for exploits, with links exposed to other attacks earlier this year with similar timelines and behavioural patterns for supply-chain attacks, such as the likes of SolarWinds, Kaseya and Juniper. SAM seamless network reported attempts to breach their systems through ‘formWsc’ and ‘formSysCmd’. Internet of Things (IoT) devices are the focus of these attacks as an entry point. Mirai malware is a botnet that focusses on IoT devices and routers and continuously evolves in its detectability and capabilities.

REMEDIATION STEPS

- Reset default passwords on IoT devices to a unique, non-guessable password.
- Use additional security features where possible such as encryption and MFA and harden configuration.
- Install firmware and operating system updates when they become available immediately.
- Ensure your network ID is not being broadcasted.
- Limit web interfaces where possible across the local network to limit the attack surface.

REFERENCES & RESOURCES

Realtek	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf
Threatpost	https://threatpost.com/attackers-exploiting-realtek/168856/