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

# CYBER GUIDANCE ISSUE 0300

## SECURITY FLAWS IN REALTEK & CACTI EXPLOITED

**DATE ISSUED:** 3rd April 2023

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | HARD | MEDIUM | **EASY** |

## OVERVIEW

Critical security flaws in Cacti, Realtek, and IBM Aspera Faspex are being exploited by various threat actors to spread ShellBot and MooBot malware capable of orchestrating Distributed Denial-of-Service (DDoS) attacks.

## BREAKDOWN

Threat actors are exploiting critical arbitrary command injection vulnerabilities in Cacti servers and Realtek Jungle SDK to distribute botnets like MooBot and ShellBot. A critical authentication bypass and command injection flaw in Cacti servers tracked as CVE-2022-46169 (CVSS score: 9.8) is being actively exploited by threat actors, which allows an authenticated user to execute arbitrary code. CVE-2021-35394 (CVSS score: 9.8) also concerns an arbitrary command injection vulnerability impacting Realtek Jungle SDK. Both flaws have been exploited by other botnet malware in the past, including Fodcha, RedGoBot, Mirai, Gafgyt, and Mozi. Once a machine is comprised, the malware downloads a script containing configuration and establishes a connection with the C2 server. It continues to exchange heartbeat messages until it recognises an incoming command to initiate a DDoS attack.

## REMEDIATION STEPS

- Use strong passwords: Implement robust password policies and two-factor authentication to prevent unauthorised access to servers and devices.
- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Keep software up to date: Keep operating systems, software applications, and plug-ins updated with the latest security patches.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

## REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/realtek-and-cacti-flaws-now-actively-exploited-by-malware-botnets/

The Hacker News https://thehackernews.com/2023/04/cacti-realtek-and-ibm-aspera-faspex.html