FORTINET

OUTBREAK ALERTS

Realtek SDK Attack

Multiple issues in Realtek SDK causing supply chain risks

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf
CVEs: CVE-2014-8361, CVE-2021-35394

FortiGuard Labs continue to see Realtek SDK vulnerabilities being exploited in the wild with over 10,000+ average IPS detections per month to deploy and distribute Denial-of-service botnet malware such as new Hinata Botnet, RedGoBot, GooberBot and Marai based Botnet.

Background

Realtek chipsets are found in many devices including, Communications Network devices, Computer Peripherals, Multimedia chips used across the industry. Two critical vulnerabilities which are actively exploited by the attackers are Realtek Jungle SDK CVE-2021-35394 which affects the 'MP Daemon' and 'UDPServer' by multiple memory corruption flaws and a relatively older vulnerability CVE-2014-8361 which affects the Realtek SDK's "miniigd" SOAP service.

Announced

At least 65 vendors are affected by the critical vulnerabilities that enable unauthenticated attackers to fully compromise the target device and execute arbitrary code. Affected devices range from network devices such as residential gateways, routers, Wi-Fi repeaters, IP cameras to smart lightning gateways and connected toys. Some of the affected vendors includes, D-Link, LG, Belkin, Zyxel, Asus, Netgear etc.

April 24, 2015: Realtek SDK miniigd RCE (CVE-2014-8361) advisory was released as 0 day.
https://www.zerodayinitiative.com/advisories/ZDI-15-155/

August 15, 2021: Realtek releases security advisory for Realtek Jungle SDK Remote Code Execution Vulnerability and provided fix for CVE-2021-35394

December 10, 2021: CISA adds Realtek Jungle SDK Remote Code Execution Vulnerability (CVE-2021-35394) to its known exploited vulnerability catalog

Latest Developments

March 20, 2023: FortiGuard Labs researchers observe high exploitation attempts of Realtek vulnerabilities CVE-2021-35394 and CVE-2014-8361 and continued ongoing attacks.

Fortinet customers remain protected by IPS signature protections and Anti-malware detections throughout the security fabric. It is recommended that users apply patches to vulnerable devices impacted by Realtek SDK flaws.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery

AV

Detects and blocks malware related to Realtek SDK Attack.

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 91.01627	DB 91.01627	DB 91.01627	DB 91.01627	DB 91.01627	DB 91.01627	DB 91.01627

FortiADC	FortiProxy
DB 91.01627	DB 91.01627

AV (Pre-filter)

Detects and blocks malware related to Realtek SDK Attack.

FortiEDR	FortiNDR
DB 91.01627	DB 91.01627

Behavior Detection

AI-based Behaviour Detection engine detects 0-day Malware

FortiSandbox
v4.0+

- Exploitation

IPS

Detects and blocks Realtek SDK Attack (CVE-2014-8361)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 21.331	DB 21.331	DB 21.331	DB 21.331	DB 21.331

Web App Security

Detects and blocks Realtek SDK Attack (CVE-2014-8361)

FortiWeb
DB 0.00345

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

FortiAnalyzer	FortiSIEM	FortiSOCaaS
DB 0.02498	DB 0.02498	DB 0.02498

Outbreak Detection

FortiAnalyzer
DB 1.00094

Threat Hunting

FortiAnalyzer
v6.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating	FortiRecon: EASM

Additional Resources

Onekey Blog	https://onekey.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/
The Hacker News	https://thehackernews.com/2023/03/new-golang-based-hinatabot-exploiting.html
Bleeping Computer	https://www.bleepingcomputer.com/news/security/malware-exploited-critical-realtek-sdk-bug-in-millions-of-attacks/

Learn more about FortiGuard Outbreak Alerts

FORTINET