F#RTINET.

# **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

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

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.

corruption flaws and a relatively older vulnerability CVE-2014-8361 which affects the Realtek SDK's "miniigd" SOAP service. 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

are Realtek Jungle SDK CVE-2021-35394 which affects the 'MP Daemon' and 'UDPServer' by multiple memory

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.

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

https://www.zerodayinitiative.com/advisories/ZDI-15-155/

2021-35394 and CVE-2014-8361 and continued ongoing attacks.

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

March 20, 2023: FortiGuard Labs researchers observe high exploitation attempts of Realtek vulnerabilities CVE-

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.



## Reconnaissance

Weaponization

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

**AV** 

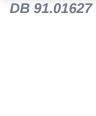
Detects and blocks malware related to Realtek SDK Attack.



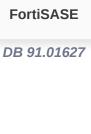


**FortiProxy** 

DB 91.01627



**FortiClient** 









**FortiCWP** 



**FortiEDR FortiNDR** DB 91.01627

Al-based Behaviour Detection engine detects 0-day Malware



**FortiSandbox** 

**FortiGate** DB 21.331

**FortiNDR** 

DB 21.331

**FortiADC** 

DB 21.331

**FortiProxy** 

DB 21.331

**FortiSASE** 

DB 21.331



DB 0.00345

Installation C2



**FortiSIEM** 

DB 0.02498

**FortiSOCaaS** 

DB 0.02498

DETECT

alert and generate reports:

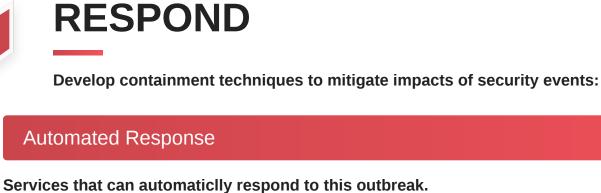
Outbreak Detection

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



### **FortiAnalyzer** v6.4+

**Threat Hunting** 



### **FortiXDR Assisted Response Services**

FortiRecon:

**RECOVER** 



Response Readiness

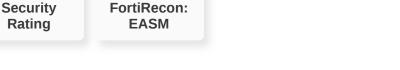
Security readiness and awareness training for SOC teams, InfoSec and general employees.

**IDENTIFY** Identify processes and assets that need protection:

Improve security posture and processes by implementing security awareness and training, in preparation for

including those introduced internally via software supply chain.

Attack Surface Monitoring (Inside & Outside)







### **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** 

**F** 

https://www.bleepingcomputer.com/news/security/malware-exploited-critical-realtek-sdk-bug-in-millions-of-attacks/

Learn more about FortiGuard Outbreak Alerts

**Announced** 

**Latest Developments** 

**Delivery** 

DB 91.01627

DB 91.01627 **Behavior Detection** 

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

Web App Security **Detects and blocks Realtek SDK Attack (CVE-2014-8361)** 

**Action** 

IOC

FortiAnalyzer

DB 0.02498





