F#RTINET. **OUTBREAK ALERTS**

TP-Link Archer AX-21 Command Injection Attack

CVEs: CVE-2023-1389

TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 contains a command injection vulnerability in the web management interface

specifically in the "Country" field. There is no sanitization of this field, so an attacker can exploit it for malicious activities and gain foothold. The vulnerability has been seen to be exploited in the wild to deploy Mirai botnet. Background

https://www.tp-link.com/us/support/faq/3643/

1389"

routers from other brands such as D-Link, DSAN and Netgear. See Additional Resources for the full report. April 27, 2023: TP-Link released a security advisory.

TP-Link is one of the global provider of WLAN devices and Archer AX21 is a Wifi router which has been used in attacks to deploy Mirai botnet. Previously we have seen Mirai based botnet attack on various other IoT devices and routers from other brands. In Feb, 2023, FortiGuard labs released a report on active attacks on vulnerable

May 1st, 2023: CISA added CVE-2023-1389 to its known exploited catalog (KEV). **Latest Developments** May 09, 2023: FortiGuard Labs released a Threat signal on vulnerability.

https://www.fortiguard.com/threat-signal-report/5157

June 20, 2023: FortiGuard Labs released a detailed blog "Condi DDoS Botnet Spreads via TP-Link's CVE-2023-

FortiGuard observed active attack attempts trying to exploit the TP-Link vulnerability (CVE-2023-1389). Fortinet customers remain protected by the IPS signature and recommends organizations to review the affected version of

the TP-Link and apply patches as recommended by the vendor as soon as possible. https://www.tp-link.com/ca/support/download/archer-ax21/v3/

https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389

PROTECT

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

Reconnaissance

Lure

events:

Detects attack attempts related to TP-Link Archer AX-21 Command Injection Attack and prevents lateral movement on the network segment

FortiDeceptor

v3.3+

Decoy VM Detects attack attempts related to TP-Link Archer AX-21 Command Injection Attack and prevents lateral movement

FortiDeceptor v3.3+ Weaponization

Detects and blocks known malware related to TP-Link Archer vulnerability (CVE-2023-1389)

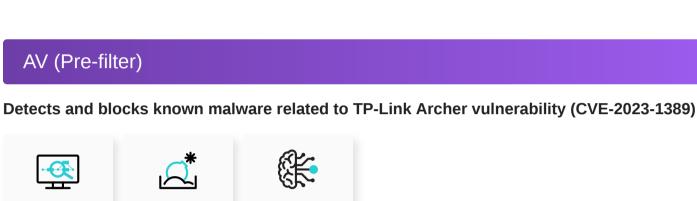
Delivery

AV

FortiCASB FortiGate FortiWeb FortiClient FortiSASE FortiMail DB 91.03531 DB 91.03531 DB 91.03531 DB 91.03531 DB 91.03531 DB 91.03531

FortiCWP

DB 91.03531



FortiProxy

DB 91.03531

DB 91.03531

Exploitation

IPS

FortiGate

DB 23.526

DB 0.00351

Installation

C2

Detects and blocks attack attempts related to TP-Link Archer vulnerability (CVE-2023-1389)

FortiADC

DB 23.526

FortiProxy

DB 23.526

FortiNDR

DB 91.03531



FortiNDR

DB 23.526

Action

DETECT

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

M.

FortiSIEM

Outbreak Detection

FortiAnalyzer FortiSIEM v6.4+ v6.4+

RESPOND Develop containment techniques to mitigate impacts of security events:

Incident FortiRecon: Response **ACI**

Assisted Response Services

RECOVER

Response **NSE Training** Readiness

Awareness & **Training**

Train your network and security professionals and optimize your incident response to stay on top of the

Additional Resources

https://www.zerodayinitiative.com/blog/2023/4/21/tp-link-wan-side-vulnerability-cve-2023-1389-added-to-the-mirai-botnet-<u>arsenal</u>

https://therecord.media/mirai-botnet-hackers-targeting-tplink

https://www.theregister.com/2023/05/02/cisa_exploited_flaws_oracle_apache/

Bleeping Computer https://www.bleepingcomputer.com/news/security/tp-link-archer-wifi-router-flaw-exploited-by-mirai-malware/ Outbreak-Router Malware Attack https://www.fortiguard.com/outbreak-alert/router-malware-attack

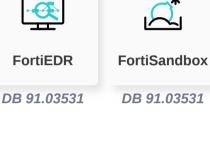
Wifi Router vulnerability actively exploited https://www.tp-link.com/us/support/faq/3643/

Announced

on the network segment

DB 91.03531

FortiADC





DB 23.526





FortiSOCaaS





FortiAnalyzer



FortiAnalyzer

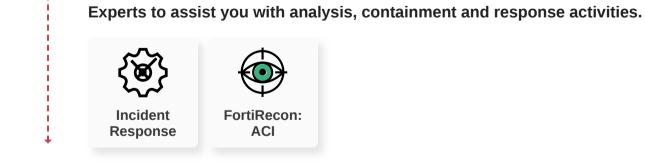
Content Update Ø.

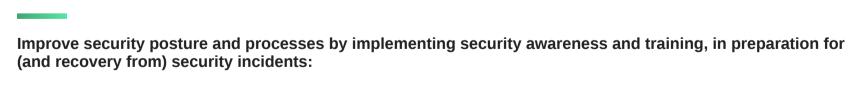
FortiSIEM

DB 316



FortiXDR

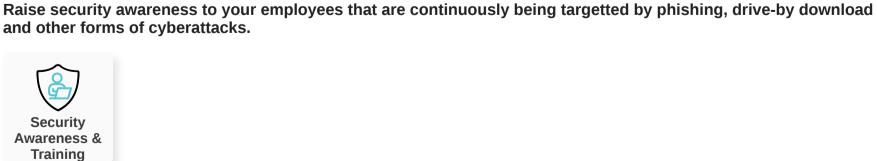




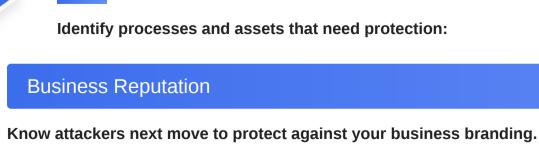
NOC/SOC Training



cyberattacks.









ZDI Research

The Record

The Register

Learn more about FortiGuard Outbreak Alerts

FEBTINET