TP-Link Cross Site Scripting

Authored by Kaustubh G. Padwad, Smriti Gaba

Posted Mar 26, 2021

Multiple TP-Link devices suffer from an unauthenticated persistent cross site scripting vulnerability. Affected models include TD-W9977, TL-WA801ND, TL-WA801N, TL-WR802N, and Archer-C3150.

tags | exploit, xss
advisories | CVE-2021-3275
SHA-256 | e35e1937104dc66eacb185dee5eb8adeeab2b99d9f05fd8364987d6dd5a729bd

Download | Favorite | View

Related Files

Change Mirror Download

```
=================================================================
Unauthenticated Stored Cross-site Scripting in Multiple TP-Link Devices
=================================================================

Overview
========

Title:- Unauthenticated Stored Cross-site Scripting in TP-Link Devices.
CVE-ID :- CVE-2021-3275
Author: Smriti Gaba, Kaustubh Padwad
Vendor: TP-LINK (https://www.tp-link.com)
Products:
1. DSL and DSL Gateway
2. Access Points
3. WIFI Routers


Tested Version: : Multiple versions of DSL & DSL Gateway, WIFI Routers and
Access Points including:

-------------------------------------------------------------------------------
Model              |    Firmware Version
    |
-------------------------------------------------------------------------------
TD-W9977           |
TD-W9977v1_0.1.0_0.9.1_up_boot(161123)_2016-11-23_15.36.15 |
TL-WA801ND         | TL-WA801NDv5_US_0.9.1_3.16_up_boot[170905-rel156404]
    |
TL-WA801N          | TL-WA801Nv6_EU_0.9.1_3.16_up_boot[200116-rel61815]
    |
TL-WR802N          | TL-WR802Nv4_US_0.9.1_3.17_up_boot[200421-rel38950]
    |
Archer-C3150       | ArcherC3150(US)_V2_170926)
    |
-------------------------------------------------------------------------------

Severity: Med-High

About the Product:
==================

* The (products from above list)  are high performance WIFI
Routers(Wireless AC routers), Access Points, ADSL + DSL Gateways and
Routers.
* Provides Configuration modes: Access Point mode, Router Mode, Range
Extender mode.
* Provide Ethernet and other interfaces to meet the access requirements of
different devices.
* It can provide high-performance functionalities, services for home users,
individual users, and businesses.
* Supports multiple functionalities including CWMP management, TR069
Configuration, SNMP management, Traffic statistics, etc.

Description:
============
An issue was discovered, common to all the TP-Link products including WIFI
Routers(Wireless AC routers), Access Points, ADSL + DSL Gateways and
Routers.
This affected TD-W9977v1,TL-WA801NDv5, TL-WA801NDv6, TL-WA802Nv5, Archer
C3150v2 devices.
A malicious XSS payload if injected in hostname of Wireless Client devices
connected to TP-Link device, allows remote attackers to execute
unauthenticated malicious scripts because of improper validation of
hostname. Some of the pages including dhcp.htm, networkMap.htm,
dhcpClient.htm, qsEdit.htm, qsReview.htm and others use this vulnerable
hostname function(setDefaultHostname()) without sanitization and push the
value of hostname ($defaulthostname) directly to the ACT stack along with
other parameters. The ACT stack is called on for multiple operation ids
covering LAN, WAN and while intialisation of multiple tables (arp, dhcp,
client list) across the device. For example, ACT_SET stack for WAN_IP_CONN
is called while dhcp operation, during which value of vulnerable
defaulthostname is being assigned to parameter X_TP_Hostname and pushed to
stack.
This causes XSS at all the endpoints which display hostname for example:
Wireless client information table, ARP bind table such as networkMap, DHCP.


Additional Information
======================
The hostname value is only validated on ASCII characters, while there is no
validation for Non-ASCII characters which allows hostname with XSS payload
say "<script>alert('XSS')</script>" to execute.
This value of hostname is pushed to an array as plain text along with IP
address and MAC address in initClientListTable() function, and other tables
use the same value of hostname accross the device. This array is then
returned to the callback function which in turn is called from proxy.js.
This data is pushed to stack corresponding to operation:"LAN_HOST_ENTRY"
(vary for different firmware), operation id: "gl" (gl is getList function).
As client initiates request with operation id:"LAN_HOST_ENTRY" and oid:
"gl", $dm.getList and $.act is called which fetches the corresponding stack
and sends data to ajax call. The crafted value of hostname is sent to the
device and results in execution of payload.


[Affected Component]
hostName parameter inside different htm pages including DHCP, DhcpAP,
ArpBind, networkMap.

-----------------------------------------
[Attack Type]
Remote
-----------------------------------------
[Impact Code execution]
true

-----------------------------------------
[Attack Vectors]
Malicious payload execution on initiating request for Wireless Client List
table or DHCP html page.

[Vulnerability Type]
====================
Stored Cross-site Scripting

How to Reproduce: (POC):
========================

    1. Change the default hostname of wireless client by using following
command (for Linux):
        a. vi /etc/dhcp/dhclient.conf
        b. Insert and change the value of hostname to xss payload
"<script>alert('XSS')</script>"
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
    2. Renew IP address by sending DHCP request to TP-Link device via
following command:
        a. vi /etc/network/interfaces
        b. Add these lines:
            auto wlan0
            iface wlan0 inet dhcp
        c. On Terminal run command: ifup wlan0
    3. Login to the router web interface, navigate to DHCP settings or
Wireless Client tab.
    4. As soon as DHCP or Wireless client table is requested Xss payload
executes and pops up alert box.

Mitigation
==========

 ------------------------------------------------------------------------------------------------------------
| Model               |   Firmware Version
      | Mitigation Comments   |
 ------------------------------------------------------------------------------------------------------------
| TL-WA801ND          | TL-WA801NDv5_US_0.9.1_3.16_up_boot[170905-rel156404]
      | Patched               |
| TL-WA801N           | TL-WA801Nv6_EU_0.9.1_3.16_up_boot[200116-rel61815]
      | Patched               |
| TL-WR802N           | TL-WR802Nv4_US_0.9.1_3.17_up_boot[200421-rel38950]
      | Patched               |
| Archer-C3150        | ArcherC3150(US)_V2_170926)
      | EOL Product           |
| TD-W9977            |
TD-W9977v1_0.1.0_0.9.1_up_boot(161123)_2016-11-23_15.36.15  | EOL Product
      |
 ------------------------------------------------------------------------------------------------------------

Link for patched software version for products:
    1. TL-WA801ND -
https://tp-link.com/beta/2021/202101/20210120/TL-WA801NDv5_US_0.9.1_3.16_up_boot[210119-rel61453].zip
    2. TL-WA801N -
https://tp-link.com/beta/2021/202101/20210120/TL-WA801Nv6_EU_0.9.1_3.16_up_boot[210119-rel62190].zip
    3. TL-WR802N -
https://tp-link.com/beta/2021/202101/20210120/TL-WR802Nv4_US_0.9.1_3.17_up_boot[210119-rel63071].zip

[Vendor of Product]
TP-LINK (https://www.tp-link.com)

Disclosure Timeline:
====================
24-July-2020 Discoverd the vulnerability
11-Aug-2020 Responsibly disclosed vulnerability to vendor
15-Aug-2020 Vendor Acknowledged the disclosure
17-Nov-2020 Communicated with vendor after 90 days for updates
19-Nov-2020 Vendor asked for model and version details
20-Nov-2020 Provided the required details to vendor
25-Nov-2020 Vendor provided software build to verify the issue
9-Dec-2020 Issue not fixed in the provided software.
4-Jan-2021 Asked Updates on the status of the issue.
20-Jan-2021 Vendor provided software build to verify the issue.
20-Jan-2021 Issue found fixed in the provided software.
21-Jan-2021 Requested for CVE-ID assignment
25-March-2021 CVE-ID Assigned.

credits:
========

* Smriti Gaba
* Security Researcher
* smritigaba548@gmail.com
* https://www.linkedin.com/in/smriti-gaba-658795135/

* Kaustubh Padwad
* Information Security Researcher
* kingkaustubh@me.com
* https://twitter.com/s3curityb3ast
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed