liyansong2018 TP-LINK Switch % ... on May 26, 2021 History

..

pictures	last year
README.md	last year

README.md

Destruction from the Percent Sign on TP-Link Smart Switch

Overview

- **CVE ID**: CVE-2021-31658
- **Type**: Out-of-bounds Read - *(125)* NULL Pointer Dereference - *(476)*
- **Vendor**: TP-LINK (https://www.tp-link.com)
- **Products**: Switch, such as TL-SG2005, TL-SG2008(US), etc.
- **Version**: 2.0 (1.0.0 Build 20180529 Rel.40524)

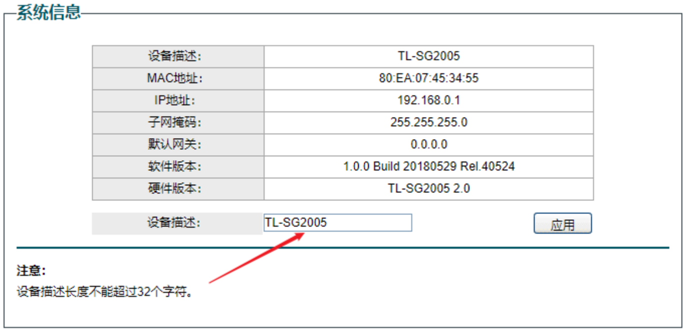
Severity

High 8.1 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

Description

The interface that provides the "device description" function only judges the length of the received data, and does not filter special characters. This vulnerability will cause the application to crash, and all device configuration information will be erased.

For example, this interface limits the length of the string entered by the user, and also limits that the name of the switch cannot contain special characters.



系统信息

设备描述:	TL-SG2005
MAC地址:	80:EA:07:45:34:55
IP地址:	192.168.0.1
子网掩码:	255.255.255.0
默认网关:	0.0.0.0
软件版本:	1.0.0 Build 20180529 Rel.40524
硬件版本:	TL-SG2005 2.0

设备描述: TL-SG2005

注意:
设备描述长度不能超过32个字符。

However, the background interface of the switch does not filter special characters. When you enter the percent sign, web process crashes, and the switch will return to factory settings.

PoC

```
http://192.168.0.1/system_name_set.cgi?sysName=%
```

Reason

- When the switch decodes the url in the background, there are two characters after the percent sign by default. So when only one character is entered, the next two non-existent characters will be read out of bounds.
- The switch uses the open source C++ library to parse the parameters returned by the front end. Open source libraries generally consider exceptions. C++ handles exceptions, while self-developed C functions (switches are embedded devices and are likely to be developed in C language) did not handle exceptions, leading to process crashes and resets.

Disclosure Timeline

- 10-Apr-2021 Discoverd the vulnerability
- 11-Apr-2021 Responsibly disclosed vulnerability to vendor
- 13-Apr-2021 Vendor Acknowledged the issue
- 16-Apr-2021 Requested for CVE-ID assignment

- 23-Apr-2021 CVE-ID Assigned
- 26-May-2021 Notify CVE about a publication