Realtek Semiconductor Corp.
No. 2, Innovation Road II,
Hsinchu Science Park, Hsinchu 300, Taiwan
Tel: +886-3-5780211; Fax: +886-3-5776047

Security Advisory

Published on: September 20, 2022

CVE	CVE-2022-40740
Title	Realtek SDK - Command Injection in GPON router WEBGUI
Description	There is a vulnerability in the authentication field of the GPON WEB page. An attacker could destroy credential configuration files via inputting the command with sign ‘&&’ to concatenate another command and then execute arbitrary commands. The root cause is that ONU does not check the format of the authentication field and filter illegal characters in the WEB Server.
Severity	High
CVSSv3	AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C/CR:L/IR:H/AR:H/MAV:L/MAC:L/MPR:H/MUI:R/MS:C/MC:H/MI:H/MA:H
Vulnerability Type	DENIAL OF SERVICE (DOS)
CWE	CWE-20 Improper Input Validation
Affected Chipsets	All Realtek xPON IC
Affected Software Versions	Realtek xPON SDK 1.9/3.3/4.0/4.1/usdk1.0/usdk2.0/usdk2.2

Acknowledgement

The Realtek Production Security Team would like to thank the following people and parties for finding and responsibly reporting security vulnerabilities to improve Realtek production security.

- Power Li < pccr10001@gmail.com >

# # #