Tenda HG6 v3.3.0 Remote Command Injection Vulnerability

Title: Tenda HG6 v3.3.0 Remote Command Injection Vulnerability
Advisory ID: ZSL-2022-5706
Type: Local/Remote
Impact: System Access, DoS
Risk: (4/5)
Release Date: 03.05.2022

Summary

HG6 is an intelligent routing passive optical network terminal in Tenda FTTH solution. HG6 provides 4 LAN ports(1*GE,3*FE), a voice port to meet users' requirements for enjoying the Internet, HD IPTV and VoIP multi-service applications.

Description

The application suffers from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the 'pingAddr' and 'traceAddr' HTTP POST parameters in formPing, formPing6, formTracert and formTracert6 interfaces.

Vendor

Tenda Technology Co.,Ltd. - https://www.tendacn.com

Affected Version

Firmware version: 3.3.0-210926
Software version: v1.1.0
Hardware Version: v1.0
Check Version: TD_HG6_XPON_TDE_ISP

Tested On

Boa/0.93.15

Vendor Status

[22.04.2022] Vulnerability discovered.
[26.04.2022] Vendor contacted.
[01.05.2022] No response from the vendor.
[03.05.2022] Public security advisory released.

PoC

tenda_hg6_cmdinj.txt

Credits

Vulnerability discovered by Gjoko Krstic - <gjoko@zeroscience.mk>

References

[1] https://packetstormsecurity.com/files/166932/Tenda-HG6-3.3.0-Remote-Command-Injection.html
[2] https://cxsecurity.com/issue/WLB-2022050009
[3] https://exchange.xforce.ibmcloud.com/vulnerabilities/225715
[4] https://sploitus.com/exploit?id=ZSL-2022-5706
[5] https://www.exploit-db.com/exploits/50916
[6] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30425
[7] https://nvd.nist.gov/vuln/detail/CVE-2022-30425

Changelog

[03.05.2022] - Initial release
[09.05.2022] - Added reference [1], [2], [3] and [4]
[13.05.2022] - Added reference [5]
[29.05.2022] - Added reference [6] and [7]

Contact

Zero Science Lab

Web: https://www.zeroscience.mk
e-mail: lab@zeroscience.mk

- **Rete mirabilia**
- **We Suggest**

- **Profiles**

- Site Meter