PTA Cyber Security Advisory No.:126 **20-01-2021**

Subject: Multiple Backdoors and Vulnerabilities found in FiberHome Routers

Summary:

Several backdoor accounts and other vulnerabilities have been discovered in the firmware of FiberHome router models HG6245D and RP2602, developed by FiberHome Networks. The available protection mechanism in the device is only available for IPv4 and IPv6 interface on the devices are vulnerable to attacks. Some of the reported security issues are listed below:

- The management interface leaks the device details if accessed from a browser with JavaScript disabled. One of the leaked details is the device's MAC address.
- A backdoor mechanism allows an attacker to use the device's MAC address to initiate a Telnet connection to the router by sending a specially crafted HTTPS request *[https://[IP]/telnet?enable=0&key=calculated(BR0_MAC)].*
- Passwords and authentication cookies for the admin panel are stored in cleartext in HTTP logs.
- The firmware also includes hardcoded credentials for managing the device via the TR-069 protocol.
- The management interface is secured through a hardcoded SSL certificate stored on the device that can be downloaded and used for MitM (Man-in-the-Middle) and other attacks.

For further details, please visit the link below:

- Multiple vulnerabilities found in FiberHome HG6245D routers - IT Security Research by Pierre (pierrekim.github.io)
- https://www.zdnet.com/article/multiple-backdoors-and-vulnerabilities-discovered-in-fiberhome-routers/

Recommendations:

- It is highly recommended to disable IPv6 till availability of IPv6 protection in the device.
- Disable unnecessary services/ ports as malware often exploit such services.
- Always security harden the devices in your organization as per industry best practices.
- Always use 2FA (Two-Factor Authentication), wherever possible.
- Update all software including Operating Systems, Servers, etc. to the latest and stable versions with appropriate patches.
- Install, regularly maintain and update Antivirus solution from a well reputed vendor.
- System Administrators/ Network Administrators to configure host-based firewalls to block outbound connections from Excel.exe, Winword.exe, Wordpad.exe, Mshta.exe, Noptepad.exe, Eqnedt32.exe and ctfmon.exe as Anti-malware solutions alone cannot fully protect against APT attacks.
- Execution of unsigned executables from sensitive webservers and endpoints must be blocked.
- Regularly provide Cyber security awareness sessions for employees and continuously arrange capacity building of the relevant technical resources.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.