ERT Threat Alert
GPON Home Routers – The Next Botnet?
May 4, 2018

Abstract

Security researchers at vpnMentor[1] recently conducted an assessment on a number of Gigabit Passive Optical Network (GPON) routers. The researchers found two exploits that could impact over one million devices and allow an attacker the ability to execute code remotely on a device. GPON is a type of Passive Optical Network (PON) used to provide fiber connections.

Background

A GPON router is a type of optical network device that is used to provide short haul fiber connections for cellular base stations, home access points and Distributed Antenna Systems (DAS). Over a million users worldwide use GPONs. Primary regions with GPON devices include Mexico, Kazakhstan and Vietnam.

vpnMentor's researchers discovered two critical GPON vulnerabilities impacting millions of home gateways. These two vulnerabilities allow an attacker the ability to bypass authentication and execute code remotely on the targeted device. This chain of exploits could result in the full compromise of a network. Following vpnMentors publications of the vulnerabilities (CVE-2018-10561 & CVE-2018-10562, CERT Kazakhstan, KZ-CERT), they issued an alert[2] after verifying the large number of GPON routers provided by telecommunication operators in the region.

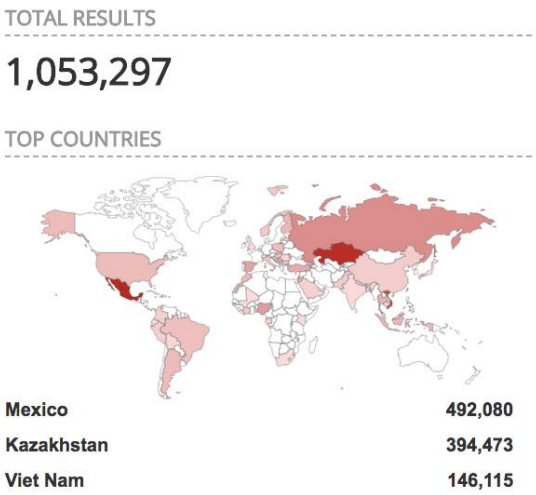

Figure 1: Top three countries with GPON home fateways

Attack Methods

Researchers at vpnMentor discovered two critical vulnerabilities that could be chained together to allow an attacker the ability to both take control of the device and the entire network. The first vulnerability, CVE-2018-10561, is an authentication bypass impacting the built-in HTTP server. This vulnerability allows an attacker the ability to change the URL in the address bar when accessing the device. By adding '`?images/`' into the end of a URL on an HTML or GponForm/ page, the attacker is able to gain access to the device. The second vulnerability, CVE-2018-10562, allows the attacker the ability to execute code remotely on the compromised device. Because the ping and traceroute commands on the diagnostics pages are at the root level, it allows other commands to be remotely executed on the device via an injection method.

**There is no information currently available about the reserved CVE's.*

[1] https://www.vpnmentor.com/blog/critical-vulnerability-gpon-router/
[2] http://kz-cert.kz/ru/page/682

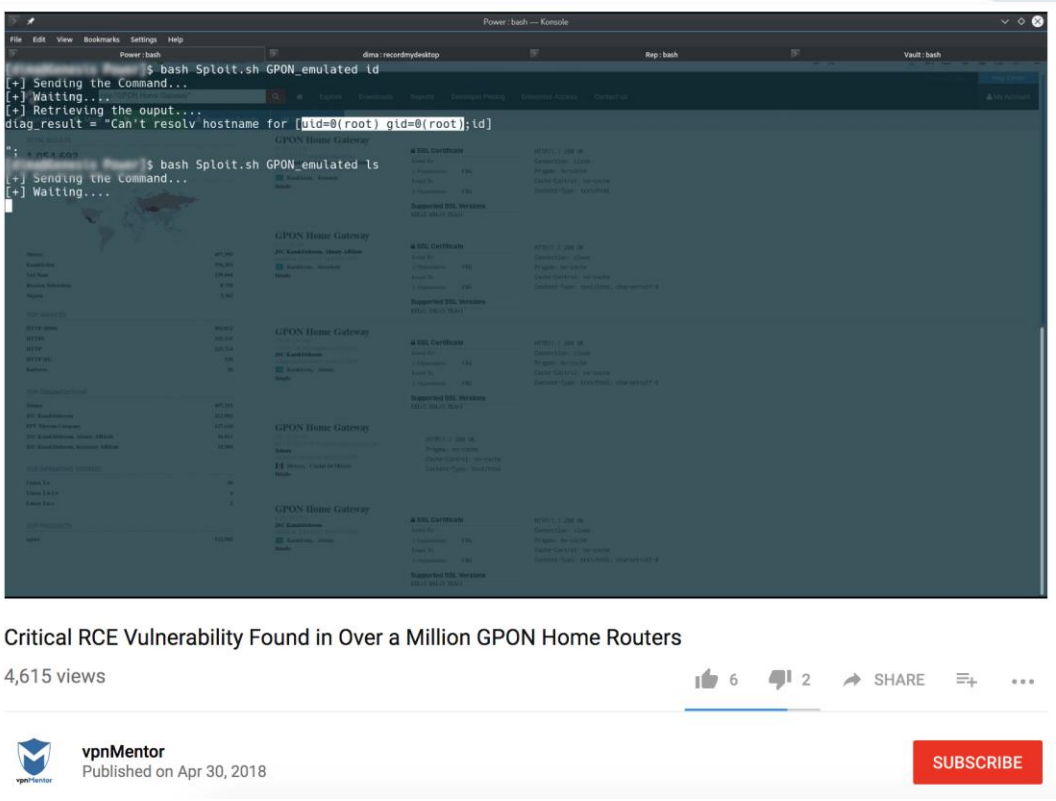

Figure 2: Video of critical RCE vulnerability in GPON home routers

Targets

Dasan Networks are a popular target since researchers and criminal hackers focus on a number of vulnerabilities found in their devices. Radware research has uncovered a new variant of the Satori Botnet - targeting port 8080 - capable of aggressive scanning and exploitation of CVE-2017-18046, an exploit of Dasan devices.

Three Reasons for Concern

1. **The Nature of Disclosure**
   The CVE's have been reserved by vpnMentor but lack information about available patches. vpnMentor has posted a video about how the exploits work, referring users to their ISP's to fix it. The concern about this disclosure is that it leaves a million estimated devices exposed with no solution to prevent these devices from being attacked.

2. **IoT Devices – Hackers' Favorite Choice**
   Due to poor built-in security features, bot herders increasingly target IoT devices, attempting to infect and control them. These devices are marketed with default credentials, open ports and other vulnerabilities. Most vendors provide no updates or patches, thereby leaving a large number of vulnerable devices.

3. **Focus on Routers and Network Switches**
   In addition to private and criminal hackers seeking to control a large botnet, state-sponsored and patriotic hackers are targeting network infrastructure, including residential routers and switches (see US-CERT advisory). Last month, a US patriotic hacker targeted routers in Russia and Iran with a defacement that displayed the message "Don't mess with our elections" with an American flag behind it. Hackers are quick to adapt and evolve, incorporating new attack vectors and exploits into their toolkits, taking control over devices to launch denial-of-service attacks, mine cryptocurrency or redirect users to phishing pages.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.