DefenseCode Security Advisory

Broadcom UPnP Remote Preauth Code Execution Vulnerability

www.defensecode.com
defensecode@defensecode.com

DefenseCode Security Advisory

http://www.defensecode.com/

Advisory ID	DC-2013-01-003
Advisory Title	Broadcom UPnP Remote Preauth Root Code Execution
Advisory URL	http://www.defensecode.com/subcategory/advisories-28
Software	Broadcom UPnP software
Vulnerable	Multiple router manufacturers
Vendor Status	Vendors contacted
Initial Release Date	2013-01-15
Release Date Postponed To	2013-01-31
Risk	Critical

1. General Overview

During the security evaluation of Cisco Linksys routers for a client, we have discovered a critical security vulnerability that allows remote unauthenticated attacker to remotely execute arbitrary code under root privileges.

Upon initial vulnerability announcement a few weeks ago Cisco spokesman stated that only one router model is vulnerable - WRT54GL.

We have continued with our research and found that, in fact, same vulnerable firmware component is also used in at least two other Cisco Linksys models - WRT54G3G and probably WRT310N. Could be others.

Moreover, vulnerability turns out even more dangerous, since we have discovered that same vulnerable firmware component is also used across many other big-brand router manufacturers and many smaller vendors.

Vulnerability itself is located in Broadcom UPnP stack, which is used by many router manufacturers that produce or produced routers based on Broadcom chipset.

We have contacted them with vulnerability details and we expect patches soon. However, we would like to point out that we have sent more than 200 e-mails to various router manufacturers and various people, without much success.

Some of the manufacturers contacted regarding this vulnerability are:

- Broadcom,
- Asus
- Cisco
- TP-Link
- Zyxel
- D-Link
- Netgear
- US Robotics
- ...and so on

Routers with vulnerable Broadcom UPnP stack are mostly based on Broadcom chipset. You can check how many manufacturers use Broadcom chipset here: http://wiki.openwrt.org/toh/start (search for Broadcom, brcm or bcm).

We don't know exactly how many of them are affected, since we were unable to contact all of them, but we suspect there are probably tens of millions vulnerable routers out there.

According to separate recent vulnerability disclosure by Rapid7 in another UPnP implementation (libupnp):

"In all, 73 per cent of problems occur with products based on four SDKs, the report found. These are Portable SDK for UPnP Devices; MiniUPnP; a third, commercial stack that is likely developed by Broadcom; and another commercial SDK that could not be tracked to a specific developer."

- Rapid7

Many routers have their UPnP interface available over the WAN interface, so the vulnerability can also be exploited over the internet. It seems that, at the moment, only popular UPnP implementation that's not hit by remote preauth security vulnerability is MiniUPnP.

2. Software Overview

Broadcom UPnP is UPnP (Universal Plug and Play) protocol implementation developed by Broadcom, and often used on routers shipped with Broadcom chipset. Vulnerability described in this advisory is located within wanipc and wanppp modules of Broadcom UPnP stack.

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

3. Vulnerability Description

During the security analysis, we have discovered remote preauth format string vulnerability in Broadcom UPnP stack. Vulnerability can be exploited to write arbitrary values to arbitrary memory address, and also to remotely read router memory. When properly exploited, it allows unauthenticated attacker to execute arbitrary code under root account.

Full exploit was previously demonstrated in the following video on Cisco Linksys WRT54GL, that is also based on Broadcom UPnP stack: http://www.youtube.com/watch?v=cv-MbL7KFKE .

Vulnerability is present in SetConnectionType function of wanipc and wanppp modules. Vulnerability itself can be reached with a single SOAP request that calls SetConnectionType function.

SetConnectionType:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope...>
<SOAP-ENV:Body>
   <m:SetConnectionType
xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1" as="">
<NewConnectionType>#FORMAT_STRING#</NewConnectionType>
   </m:SetConnectionType>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Format string output is available through GetConnectionTypeInfo SOAP request as presented below.

GetConnectionTypeInfo:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope...>
<SOAP-ENV:Body>
   <m:GetConnectionTypeInfo
xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1">
   </m:GetConnectionTypeInfo>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Format string vulnerability is present because user-input from SOAP request is supplied as a format string argument to the snprintf() function in files wanipc.c and wanpp.c. Vulnerable code lines are located in the following files and code lines:

/upnp/igd/wanipc.c:

```
static int SetConnectionType(UFILE *uclient, PService psvc, PAction ac,
pvar_entry_t
args, int nargs) {
     snprintf(psvc->vars[VAR_ConnectionType].value, sizeof(psvc-
>vars[VAR_ConnectionType].value), ac->params[0].value);

     return TRUE;
}
```

/upnp/igd/wanppp.c:

```
int WANPPPConnection_SetConnectionType(UFILE *uclient, PService psvc,
PAction ac,
pvar_entry_t args, int nargs)
/*     "SetConnectionType", WANPPPConnection_SetConnectionType, */
{
     snprintf(psvc->vars[VAR_ConnectionType].value,
sizeof(psvc->vars[VAR_ConnectionType].value), ac->params[0].value);

     return TRUE;
}
```

4. Solution

Since vulnerability is spread across multiple router manufacturers, and we were unable to reach all of them on this matter, it's unclear how long it will take certain manufacturers to patch it. Especially those that we were unable to contact. However, we're open to any questions from vendors regarding this vulnerability.

Moreover, during the contact with one particular vendor, we were asked if the vulnerability is in *<name-intentionally-removed>* function. It wasn't. But that quickly led us to yet another vulnerability in also popular router software, obviously already reported to router manufacturers by someone, but still non-public.

ADVISORY UPDATE: That turns out to be libupnp vulnerability disclosed by Rapid7.

5. The Exploit

We have developed working exploit as demonstrated in video http://www.youtube.com/watch?v=cv-MbL7KFKE , but because of the vulnerability impact and presence of this vulnerability across multiple router manufacturers, we won't publish the exploit.

6. Credits

Vulnerability discovered by Leon Juranic and Vedran Kajic. We would like to thank Kost for further help on shellcode development, and Davor Serfez for router debugging. Also, thanks to Armijn Hemel for helping us contacting some router manufacturers.

7. About DefenseCode

DefenseCode is an information security consultancy company. DefenseCode provides security services and products designed for comprehensive security assessment of web applications, network and software products. DefenseCode is specialized in web application security and provides both static source code security analysis and dynamic web application security analysis security products.

DefenseCode security products are designed for comprehensive security audit of web applications. Audit your web applications for SQL Injections, Cross Site Scripting, Code Execution, File Inclusion, and much, much more.

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com