

[Full-disclosure] RLA ("Remote LanD Attack")

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-12/msg00606.html>

- *From:* Synister Syntax <synistersyntaxlist@xxxxxxxxx>
 - *Date:* Wed, 14 Dec 2005 01:49:28 -0500
-

Below is a copy of my RLA exploit submission in ASCII. Attached is a MSWord (.doc) version with rich formatting, created with ease of view in mind.

Regards...

RLA
("Remote LanD Attack")
2005

As discovered by:
Justin M. Wray
(jayzkool@xxxxxxxxx)

Devices/Vendors Vulnerable:

- Microsoft Windows XP, SP1 and SP2
- Linksys Routers
- Westell Routers/Modems
- Motorola Modems/Routers
- Cisco Firewalls, Switches, and Routers
- DSL Modems
- Cable Modems
- Consumer Routers
- All Central Connectivity Devices (any manufacturer)

Devices/Vendors Tested:

- Linksys BEFW11S4
- Linksys WRT54GS
- Westell Versalink 327W (Verizon Modem)
- Cisco Catalyst Series (Multiple)
- Scientific Atlantic DPX2100 (Comcast Modem)

Definition:

A LAND attack is a DoS (Denial of Service) attack that consists of sending a special poison spoofed packet to a computer, causing it to

[Full-disclosure] RLA ("Remote LanD Attack")

lock up. The security flaw was first discovered in 1997 by someone using the alias "m3lt", and has resurfaced many years later in operating systems such as Windows Server 2003 and Windows XP SP2. (http://en.wikipedia.org/wiki/LAND_attack)

Explanation of LanD:

LanD uses a specially crafted ICMP echo packet which has the same source and destination address. The receiving system stalls due to the erroneous packet and not having instructions to handle the unique packet. In Windows 9x variants, the systems will "blue screen. " On modern NT variants, the systems will hang for approximately 30 seconds with full CPU usage before discarding the packet. With a looped script, the attacker can render the system useless. UNIX variants have been able to use a firewall rule to drop LanD packets leaving most systems patched.

Microsoft originally released an initial patch that secured Windows 9x variants causing the exploit to lose popularity and become somewhat obscure. Later, when Windows NT variants were released, Microsoft neglected to patch the security flaw; this caused Windows XP Service Pack 2 to remain susceptible to such an attack. Within the last four (4) months, Microsoft has released a patch for Windows NT variants.

LanD versus Remote LanD:

LanD was originally introduced in the late 1990s and was very popular with educational and business networks. The original LanD attack had to be executed internally on the local network thereby giving rise to the name "LanD" (indicating that access has been granted to the local premises). However, with a remote attack (Remote LanD), crafting special packets and spoofing the destination and source IP addresses will cause the attack to be carried out remotely against the central connectivity device.

Exploit / Proof of Concept:

There is no handwritten code needed to exploit this vulnerability. The only requirement is an IP packet creation utility (such as HPing2 or IPSorcery). Below are some HPing2 examples:

Victim's IP Address: 63.24.122.59

Victim's Router IP Address: 192.168.1.1

```
hping2 -A -S -P -U 63.24.122.59 -s 80 -p 80 -a 192.168.1.1
```

Remote LanD Specifications:

Although the exploit will work without the Ack, Syn, Push, and Urg (flags), the device does not seem to shut off without these flags.

Sending just the LanD part of the packet seems to only create high amounts of latency on the victim's end. The spoofed source address must be the address of the central connectivity device; although the normal default is 192.168.1.1, some manufacturers use different addresses (such as 192.168.1.100 or 192.168.0.1). As a result, the IP address should be checked prior to initiating any test. Additionally, a broadcast address will work for a source address as well, thereby

[Full-disclosure] RLA ("Remote LanD Attack")

flooding the network with responses from all the machines connected to the network. Although it will not stale the Central Connectivity Device, it will maximize the entire network usage – crippling the network with extremely high latency.

Test Environment:

- Test One
- Attacker: hping2 on Comcast Cable connection behind Linksys Router
- Victim: DSL Modem/Router on Verizon DSL connection

- Test Two
- Attacker: hping2 on Comcast Cable connection behind Linksys Router
- Victim: Linksys Router on Comcast Cable connection

- Test Three
- Attacker: hping2 on Comcast connection behind Linksys Router
- Victim: Comcast Cable Modem

- Test Four
- Attacker: hping2 on Comcast connection behind Linksys Router
- Victim: Cisco Router on T1 connection

- Test Five
- Attacker: hping2 on Comcast connection behind Linksys Router
- Victim: Cisco Pix Firewall, on T1 connection

Test Results:

Test One:

Connection Latency – followed by the modem physically turning off. Time elapsed: approximately 10 seconds (from beginning of packet flooding to complete shutdown).

Test Two:

Connection Latency, router reset, then connection lost. Reset needed before router would communicate online again.

Test Three:

Modem lights flickered; the modem lost connection and sat with the Data light completely out.

Test Four:

Router lost connection to the internet.

Test Five:

Firewall lost network connection.

Conclusion:

It appears that central connectivity device manufacturers need to release firmware updates and/or patches to protect against LanD and remote LanD attacks. The LanD attack is no longer simply a local

[Full-disclosure] RLA ("Remote LanD Attack")

attack but has now evolved into having the capability of being launched remotely.

Acknowledgements:

- Casey O'Brien, M.S.
- Assisted with test trials
- Matthew Wines
- Assisted with test trials
- Yvonne M. Wray, M.S.
- Report editor

Submitted: 12/14/2005 by Justin M. Wray

--

Regards,
SynSyn
Network Manager, Server Administrator, Security Specialist
(<http://www.teamtrinux.com>)

Attachment: RLA.doc

Description: MS-Word document

Full-Disclosure - We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia - <http://secunia.com/>