WIKIPEDIA

LAND

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

Contents

Mechanism

The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. This causes the machine to reply to itself continuously. It is, however, distinct from the TCP SYN Flood vulnerability.

Other LAND attacks have since been found in services like SNMP and Windows 88/tcp (kerberos/global services). Such systems had design flaws that would allow the device to accept request on the wire appearing to be from themselves, causing repeated replies.

Vulnerable systems

Below is a list of vulnerable operating systems:[1]

- AIX 3.0
- AmigaOS AmiTCP 4.2 (Kickstart 3.0)
- BeOS Preview release 2 PowerMac
- BSDi 2.0 and 2.1
- Digital VMS
- FreeBSD 2.2.5-RELEASE and 3.0 (Fixed after required updates)
- HP External JetDirect Print Servers
- IBM AS/400 OS7400 3.7
- Irix 5.2 and 5.3
- Mac OS MacTCP, 7.6.1 OpenTransport 1.1.2 and 8.0
- NetApp NFS server 4.1d and 4.3

- NetBSD 1.1 to 1.3 (Fixed after required updates)
- NeXTSTEP 3.0 and 3.1
- Novell 4.11
- OpenVMS 7.1 with UCX 4.1-7
- QNX 4.24
- Rhapsody Developer Release
- SCO OpenServer 5.0.2 SMP, 5.0.4
- SCO Unixware 2.1.1 and 2.1.2
- SunOS 4.1.3 and 4.1.4
- Windows 95, NT and XP SP2,

Prevention

Most firewalls should intercept and discard the poison packet thus protecting the host from this attack. Some operating systems released updates fixing this security hole. In addition, routers should be configured with both ingress and egress filters to block all traffic destined for a destination in the source's address space, which would include packets where the source and destination IP addresses are the same.

See also

- Slowloris (computer security)
- High Orbit Ion Cannon
- Low Orbit Ion Cannon
- ReDoS
- Denial-of-service attack

References

1. http://insecure.org/sploits/land.ip.DOS.html

External links

- Insecure.Org's original post about the attack (http://insecure.org/sploits/land.ip.DOS.html)
- Article about XP's vulnerability (http://www.internetnews.com/security/article.php/3488171)
