US-CERT Federal Informational Notice FIN05-095

4.5.05

Default implementations of IPv6 may present a security risk and present perimeter detection issues for Federal agencies.

OVERVIEW

While the IPv6 standard has yet to be widely deployed in the Federal space, there exist several potential security risks that must be properly recognized and managed. IPv6 presents unique challenges to network security monitoring and perimeter protections afforded by edge devices (i.e., router access-lists or firewalls) and many intrusion detection systems. While in some instances IPv6 is more secure than IPv4, additional security considerations are warranted in order to understand how network threats may be associated with IPv6 implementations.

This Federal Information Notice should serve all agencies as a starting point for further investigation into current and future deployment strategies for IPv6 use within Federal networks.

DESCRIPTION

IPv6 was initially designed to alleviate the address space limitations of IPv4 and provide additional security and routing capabilities. IPv4 provides 4.29 billion addresses and IPv6 provides nearly 600 quadrillion addresses for every square millimeter on earth.[1] Most current operating systems now support IPv6 by default. As a result, the following security risks may be unknowingly introduced: auto-configuration and the subsequent tunneling of IPv6 traffic through Federal networks.

One feature of IPv6 is auto-configuration where a device that is IPv6 enabled will derive its own IP address from neighboring routers without an administrator's intervention. Further, the device may solicit and accept advertisements to route IPv6 traffic. No DHCP server is required for the device to assign itself an IP address, which is a characteristic of IPv4 deployments. Please note that the auto configuration of the link local addressing is a separate issue from the auto configuration of additional addresses accepted via IPv6 router advertisements.

Tunneling is the ability to send traffic of one kind across a network encapsulated within an additional protocol. While there are legitimate purposes for tunneling (i.e., NetBios over IPv4), there exists the possibility that traditional IDS or firewall devices will be not configured to recognize that traffic stream, and therefore the protection those devices provide may be bypassed. A malicious external user or compromised internal host could send crafted IPv6 packets, which might pass undetected (and unblocked) through perimeter security devices (i.e., firewalls or router access-lists). Also, there has been a recent increase of malicious code that will enable IPv6 on a compromised host, which will allow a potentially undetected channel for an attacker to exploit.

IMPACT

Unmanaged or rogue implementations of IPv6 present a network management security risk to network administrators when devices automatically configure themselves with an IPv6 address without authorization. In addition, since some firewalls and/or IDS products do not provide IPv6 detection of filtering capability malicious users might be able to tunnel an IPv6 packet through these security devices undetected. Reconnaissance activity inbound (e.g., port scanning) or communication traffic outbound (e.g., botnet activity) could be facilitated in a network that does not control their IPv6 implementation.

RECOMMENDATIONS

While there is no formal documentation that may provide guidance for Federal agencies considering the deployment of IPv6, it is advised that Federal network professionals consult NIST special publication 800-65 to adequately assist in the integration of IT security into their long term planning and deployment strategy.

The solutions outlined by Sean Convery and Darrin Miller in their paper "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)" provides industry best practices from a Cisco perspective. Federal network architects and network security professionals should carefully review and seek additional resources before selectively applying any recommendations to their network.

US CERT recommends in the short term the following:

- IPv6 perimeter controls should be first implemented at the edge filtering devices
- Determine if firewalls and IDS products support IPv6 and implement additional IPv6 security measures
- Determine IPv6 devices and disable if not necessary
- Disable IPv6 via use of standard configurations and/or with configuration management tools (e.g., group policy within Windows 2000/2003 environments)

Recommendations detailed within the whitepaper:

- Filter internal-use IPv6 addresses at organization border routers
- Use standard, but non-obvious static addresses for critical systems
- Filter unneeded services at the firewall
- Selectively filter ICMP
- Maintain host and application security

Additional security recommendations for firewalls:

- Determine what extension headers will be allowed through the access control device
- Determine which ICMPv6 messages are required

To handle fragmentation attacks:

- Deny IPv6 fragments destined to an internetworking device when possible
- Ensure adequate IPv6 fragmentation filtering capabilities
- Drop all fragments with less than 1280 octets (except the last one)

To address spoofing attacks:

- Implement RFC 2827-like filtering and encourage your ISP to do the same
- Document procedures for last-hop traceback
- Use cryptographic protections where critical

To address routing attacks:

- Use traditional authentication mechanisms on BGP and IS-IS
- Use IPsec to secure protocols such as OSPFv3 and RIPng

To address worm and virus attacks:

- Implement IPv4 best practices to include timely patching, host antivirus, and early detection followed by perimeter blocking

To address tunneling attacks:

- Use dual stack as your preferred IPv6 migration choice
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

SYSTEMS AFFECTED

Any device with IPv6 enabled or supported. Please note that many operating systems (see below) have IPv6 enabled by default.

Please reference your individual operating system and networking device vendors or manufacturers for further guidance.

Below is a list of commonly installed operating systems and devices that support IPv6 and when applicable it is noted if a system enables IPv6 by default. A more detailed list can be found at http://www.ipv6.org/.

Macintosh

- Mac OS X 10.2 Jaguar (IPv6 built-in)

Unix

- AIX 4.3 and later (IPv6 enabled by default)
- BSDI BSD/OS v4.0 and later (IPv6 enabled by default)

- Compaq Tru64 UNIX [formerly known as DIGITAL UNIX] (IPv6 enabled by default)
- FreeBSD 4.0 and later (integrates KAME IPv6 stack and has IPv6 enabled by default), it does not accept router advertisements by default, however it does auto configure IPv6 link local addresses.
- IRIX SGI and later (currently not implemented but customers with support licenses can request beta software)
- Linux kernel version 2.2 and above (IPv6 built-in)
- NetBSD 1.5 and later (IPv6 built-in)
- OpenBSD 2.7 and later (integrates KAME IPv6 stack and IPv6 is enabled by default), it does not accept router advertisements by default, however it does auto configure IPv6 link local addresses.
- Solaris 8 and later (IPv6 built-in)
- HP-UX 11i IPv6 and later (available via Transport Optional Upgrade Release (TOUR) 2.0 upgrade)

Windows

- Windows 95/98/NT (IPv6 support available but not built-in)
- Windows 2000 (add-on available for IPv6)
- Windows XP (IPv6 built-in)
- Windows Server 2003 (IPv6 built-in)

Other OS

- OS/390 IBM formerly MVS (IPv6 supported but not built-in)
- Compaq OpenVMS V5.1 (IPv6 built-in)
- z/OS (IBM's current mainframe operating system) includes ipv6 support beginning with v1.4 , although it is disabled by default. Once enabled, its auto configuration includes accepting router advertisements.

Routers

- Cisco (supports IPv6 since IOS 12.2(2)T)
- Hitachi (hardware is available with IPv6 supported)
- Nortel Networks has IPv6 support in some routers
- Juniper Networks has IPv6 in some of their routers
- 6wind builds IPv6 routers
- IIJ SEIL series builds IPv6 routers
- Yamaha RT routers support IPv6

CREDITS and REFERENCES

Information from the following sources was used in the preparation of this notice (URLs may be wrapped for readability).

- "IPv6: The Next Generation Internet (http://www.ipv6.org/)
- Windows XP (http://www.microsoft.com/technet/prodtechnol/winxppro/plan/faqipv6.mspx)
- Windows Server 2003 (http://www.microsoft.com/windowsserver2003/technologies/ipv6/default.mspx)
- Windows 95/98/NT (http://www.trumpet.com.au/ipv6.htm)
- Cisco (http://www.cisco.com/warp/public/732/Tech/ipv6/)
- Quick-start IPv6 HOWTOs (http://www.ipv6.org/howtos.html)
- Sean Convery and Darrin Miller - "IPv6 and IPv4 Threat Comparison and Best PracticeEvaluation (v1.0)"
- US-CERT VU#658859 "Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 memory leak (http://www.kb.cert.org/vuls/id/658859)
- US-CERT VU#472582 "Cisco IOS IPv6 denial-of-service vulnerability (http://www.kb.cert.org/vuls/id/472582)

---

[1] http://www.rtcmagazine.com/home/printthis.php?id=100022

Last updated April 05, 2005