CNS /Update Newsletter Feature

Security Corner: Pilot for New Private IP Standard Launched

CNS Document ID: u040109a
Last Updated: 1/13/04

UF Information Technology

UFIT
2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Security Corner: Pilot for New Private IP Standard Launched ......................................3

Table of Contents

Security Corner: Pilot for New Private IP Standard Launched .................................3
Security Corner: Pilot for New Private IP Standard Launched

A new private Internet Protocol (IP) standard has been implemented for UF, according to Jordan Wiens, network security engineer for CNS. "Call it PIP, for 'Private Internet Protection,'" says Wiens. "This new standard will help us protect private IP addresses, which previously have been vulnerable to Internet threats."

Blocks of IP address space in certain number ranges are reserved for private (home, company, or campus) intranets. IP addresses in these ranges may be freely assigned on local networks because they are not allowed on the public Internet. To connect to the public Internet, the address must be translated to a temporary public address. The most common standard is Network Address Translator, or NAT. Private IP is often used for workstations and for wireless and walk-up networks. With the increasing use of these devices comes an increasing number of workstations exposed to Internet threats. This creates a serious risk to UF IT resources.

The new IP standard that has been implemented at UF protects private IP address space from security compromises. To minimize exposure, translated private IP connections outside the UF network will be restricted to those initiated by the internal host: our solution allows only connections that the user initiates.

Private IP was introduced to help manage Internet growth and reduce the load on IPv4 address space. It evolved to become a mechanism for providing security to private hosts. The UF private IP standard states that 10.0.0.0/8 addresses are translated one for one to public addresses when a private host attempts to access external Internet resources. This means that as soon as a private address accesses an external Internet resource, the private address is translated to a public address that is openly exposed to Internet threats.

Some exceptions for virus updates and other legitimate active FTP traffic will be made.

Transferring files with some applications will not work if they require communication to be initiated by an external host on a different port. You may need to find another way to accomplish transferring of files for some instant direct user-to-user messaging applications, network meeting applications, and video conferencing applications.

For more information, see http://net-services.ufl.edu/security/admins/private-ip-std.shtml.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT