

ResNet Security Plan for Windows RPC Vulnerability August 14, 2003

IT Security & Policy along with IT Telecommunications have implemented the ResNet Security Plan to help address current threats to ResNet machines such as:

- Listing of systems, shares and users accounts
- Worms and viruses
- Accidental sharing of information
- Theft of information from ResNet machines
- Use of ResNet machines by hackers to attack other computers/networks

In an effort to control the spread of the Blaster/Lovesan worm that resulted from the Windows RPC vulnerability, we will also be temporarily implementing an outbound block on port 135 for the ResNet subnets. This outbound block for port 135 is in addition to the ResNet Security Plan already in place for this fall. For more information about the ResNet Security Plan, go to <http://www.itap.purdue.edu/security/policies/resnet/>.

The outbound block on port 135 will be in place until we can determine that ResNet computers are patched and any infected machines are fixed and patched. We expect this will be necessary for the short term, possibly only for a few weeks.

Some services may not function due to this outbound block. We anticipate users may see problems with Microsoft Exchange calendaring, drive mapping, and other RPC related services. Mapping drives to Rosetta for access to home directories will not be affected by this block.

ResNet staff will be available to assist users with patching and cleaning up their computers. If you need assistance in patching your computer or removing the worm, please send e-mail to resnet@purdue.edu. If you have other security-related questions, please send e-mail to itap-securityhelp@purdue.edu.

For more information about the Windows RPC vulnerability and the Blaster/Lovesan worm see the Headlines on the IT Security & Policy web page at <http://www.itap.purdue.edu/security/>.