

Sygate Security Bulletin ID SS20030129-0002

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-01/0062.html>

From: Elisha Riedlinger (elisha.riedlinger@SYGATE.COM)

Date: 01/31/03

Date: Thu, 30 Jan 2003 18:19:23 -0800
From: Elisha Riedlinger <elisha.riedlinger@SYGATE.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Sygate Security Bulletin

Sygate was made aware of an exposure in Sygate Personal Firewall 5.0 and Sygate Security Agent 3.0 on 1/23/2003 by David Fernandez Madrid (conde0@telefonica.net).

Sygate Security Bulletin ID

SS20030129-0002

Description

The reporter of the vulnerability described a problem in which a remote attacker could gain access to a system with an open UDP port that was protected by Sygate Personal Firewall by sending specially crafted UDP packets in an attempt to bypass the firewall.

Impact of this vulnerability

Systems are not vulnerable to attempts by remote attackers to gain access to open UDP ports and bypass Sygate Personal Firewall or Sygate Security Agent if the attacker is on a different network than the system running Sygate Personal Firewall or Sygate Security Agent and NetBIOS Protection is enabled.

If an attacker is on the same IP subnet as the system protected by Sygate Personal Firewall or Sygate Security Agent, or if NetBIOS Protection is disabled, this vulnerability can be taken advantage of.

Affected software

- * Sygate Personal Firewall Pro 5.0
- * Sygate Personal Firewall 5.0
- * Sygate Security Agent 3.0

Vulnerability resolution

This vulnerability condition pertaining to an attacker on a local network gaining access to open UDP ports and bypassing Sygate Personal Firewall or Sygate Security Agent is addressed by adding new firewall rules.

Instructions

for adding the new rules are detailed below.

In conformance with RFPolicy, Sygate has created a security@sygate.com email address to supplement the previously existing security-alert@sygate.com email

address. Additionally the policies for handling vulnerability advisories regarding Sygate products have been re–examined and improved to facilitate better communication between researchers and Sygate, Inc.

Users of Sygate Personal Firewall should use the following instructions to add

the NetBIOS name service and NetBIOS datagram service rules under the Advanced

Rule Editor:

For NetBIOS name service, use the following instructions to add a rule for port 137:

- 1) Select the Add button.
- 2) Enter Microsoft SQL Monitor Service as the Rule Description
- 3) Select the Block this traffic radio button
- 4) Select All network interface cards under Apply Rule to Network Interface
- 5) Select Both on and off under Apply this rule during Screensaver Mode
- 6) Select the Hosts tab at the top of the Advanced Rule Settings window
- 7) Select All Addresses under Apply this rule to
- 8) Select the Ports and Protocols tab at the top of the Advanced Rule Settings Window
- 9) Select UDP under Protocol
- 10) Select NETBIOS–NS(137) under Remote
- 11) Manually enter 0–136,138–65535 under Local
- 12) Select Both under Traffic Direction
- 13) Select the Ok button

For NetBIOS Datagram service, use the following instructions to add a rule for port 138:

- 1) Select the Add button.
- 2) Enter NetBIOS Datagram Service as the Rule Description
- 3) Select the Block this traffic radio button

- 4) Select All network interface cards under Apply Rule to Network Interface
- 5) Select Both on and off under Apply this rule during Screensaver Mode
- 6) Select the Hosts tab at the top of the Advanced Rule Settings window
- 7) Select All Addresses under Apply this rule to
- 8) Select the Ports and Protocols tab at the top of the Advanced Rule Settings Window
- 9) Select UDP under Protocol
- 10) Select NETBIOS–DGM(138) under Remote
- 11) Manually enter 0–137,139–65535 under Local
- 12) Select Both under Traffic Direction
- 13) Select the Ok button

System Administrators of Sygate Management Servers providing configurations to systems running Sygate Security Agent should use the following instructions to add rules to protect their systems:

- 1) Select the Policies tab
- 2) Select the Simple Rules sub tab
- 3) Check out group for the new rule (repeat for additional groups or select the Global group to effect all groups)
- 4) Ensure Active Directory Sharing and Network Neighborhood Sharing are not enabled
- 5) Select the Advance Rules sub tab
- 6) Expand the list of locations
- 7) Select a location for the new rule (repeat for additional locations)
- 8) Expand the Security icon to display the list of available adapters
- 9) Select All Adapters under the list of available adapters
- 10) Enter Allow NetBIOS Browsing as the Rule Description
- 11) Select the Add button
- 12) Select the Allow NetBIOS Browsing rule listed under All Adapters
- 13) Select the Applications tab listed under Events and Triggers
- 14) Select a Priority and Severity level that is appropriate to your network environment such as Priority: 13, Severity: 10
- 15) Select Enable Application Triggers by placing a check in the checkbox
- 16) Select the Add button
- 17) Enter NT OS Kernel as the Application Description
- 18) Enter ntoskrnl.exe as the file name
- 19) Select Create Application Fingerprint by placing a check in the checkbox
- 20) Select the Ok button
- 21) Select the Add button again
- 22) Enter Windows OS Kernel as the Application Description
- 23) Enter kernel32.dll as the file name
- 24) Select Create Application Fingerprint by placing a check in the checkbox
- 25) Select the Ok button
- 26) Select the Services tab listed under Events and Triggers

