

ESM Response Policy Release Notes

Unchecked Buffer in Universal Plug and Play
for Windows XP operating systems



ESM Response Policy Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2001 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Enterprise Security Manager are trademarks of Symantec Corporation.

Windows and Windows NT are registered trademarks or trademarks of Microsoft Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

Windows XP Unchecked Buffer Response Policy Release Notes

Introducing response policies	3
Windows XP Unchecked Buffer response policy	4
How ESM identifies vulnerable Windows XP systems	4
Policy installation procedures	5
Installation prerequisites	5
Installation steps	5

Service and support solutions



Windows XP Unchecked Buffer Response Policy Release Notes

This document contains release notes for the Unchecked Buffer in Universal Plug and Play response policy for Enterprise Security Manager® (ESM) agents on Windows XP operating systems.

The Windows XP Unchecked Buffer response policy checks Windows XP operating systems to determine whether these systems are exposed to the vulnerabilities described in Microsoft Security Bulletin MS01-059.

Introducing response policies

ESM response policies are configured by members of the Symantec Security Response team to respond to recent security incidents and newly-detected security vulnerabilities without waiting for scheduled module Security Update releases.

Response policy names are identified and sorted by “R-” prefixes in the Policies branch of the ESM Enterprise tree in the ESM Console.

Windows XP Unchecked Buffer response policy

The Windows XP Unchecked Buffer response policy identifies Windows XP systems that have not had their Universal Plug and Play (UPnP) patched to avoid the vulnerabilities described in Microsoft Security Bulletin MS01-059.

Microsoft Security Bulletin MS01-059 describes a remotely exploitable buffer overflow in the UPnP application that is installed and enabled by default on Windows XP workstations. Remote users can send UDP packets to vulnerable systems that will cause buffer overflows and other denial of service attacks. For more information on these vulnerabilities, see <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-059.asp>.

How ESM identifies vulnerable Windows XP systems

The Windows XP Unchecked Buffer response policy uses the ESM OS Patches module to identify Windows XP systems that are vulnerable to the UPnP buffer overflow. The OS Patches module enables the universalpnp.pwx template file to check your Windows XP systems for Microsoft patch Q315000, "Windows XP Security Patch: Unchecked Buffer in UPnP can lead to system compromise," which was released in December, 2001. The module identifies systems that are running this patch by looking at the file dates of the Ssdpapi.dll, Ssdpsrv.dll, upnp.dll and netsetup.exe files.

Policy installation procedures

The Windows XP Unchecked Buffer response policy should be installed on ESM 5.5 managers that will run the policy on Windows XP agents.

Note: If you intend to run this policy on Windows XP agents, these agents should be registered to the manager before you install the response policy.

Installation prerequisites

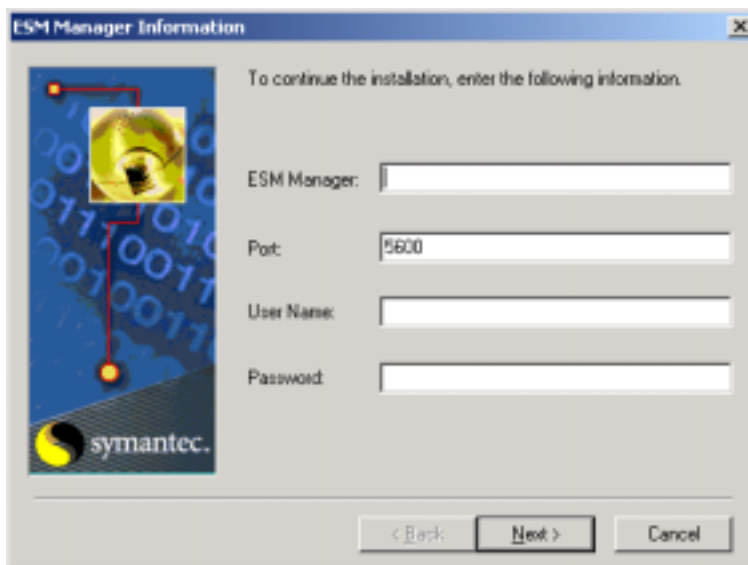
Before you run the executable program that installs the security response policy that is documented in these Release Notes, you must complete the following prerequisites:

- Upgrade all ESM manager and agent systems that will use the security response policy to ESM version 5.5.
- Upgrade the modules on all ESM manager and agent systems that will use the security response policy to Security Update 10 or later.
- Download the Unchecked Buffer in Universal Plug and Play response policy from <http://securityresponse.symantec.com>.
- Identify the ESM account name, the ESM account password, and the communication port that you will need to use to connect to each ESM manager you intend to install.

Installation steps

- 1 Run the Response_WindowsXP_Universal PnP_20011220.exe executable file from a Windows NT, 2000, or XP system that has network access to the ESM manager you want to install.
- 2 Click **Next** to close the InstallShield Welcome dialog box.

- 3 If the installation program does not find the required Java™ 2 Runtime libraries on your system, you will be prompted to install the Java 2 Runtime Environment. Click **Yes** to start the installation, click **Yes** to accept the Software License Agreement, and then click **Next** to install the Java 2 Runtime Environment.
- 4 Click **Yes** to continue installation of the security response policy.



- 5 Enter requested ESM Manager Information, then click **Next**.

Note: If ESM does not find an agent with the required operating system or ESM security update version on the specified manager, the install program returns an error message and aborts the installation of the security response policy. To resolve this error, register an agent with the required application and operating system and install the latest module security update; then rerun the install program.

- 6 Click **Finish** to exit the installation program after a successful installation.

S U P P O R T

Service and support solutions

Symantec's Technical Support Group of skilled Technical Engineers can provide platform-specific information about Symantec products. Our staff has in-depth expertise in both client/server computing and information security technology.

Contacting Technical Support

To contact Symantec's technical support:

North America, Latin America, or Asia Pacific

Telephone: **(888) 727-8671**

Web: <http://www.symantec.com/techsupp/>

Outside North America but supported from the United States (i.e., APLA)

Telephone: **(781) 663-2686**

Web: <http://www.symantec.com/techsupp/>

Europe, Middle East, Africa, (EMEA)

Telephone: **+44 (0) 1372 214321**

FAX: **+44 (0) 1372 751815**

E-mail: eurbox_epsom@symantec.com

Licensing

Telephone: **(888) 584-3925**

FAX: (781) 487-9818

E-mail: license@symantec.com

World Wide Web Site

Web: <http://www.symantec.com/techsupp/>

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

<http://www.symantec.com/>
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina, Chile, and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

<http://www.symantec.com/region/mx>
+54 (11) 4315-0889
Fax: +54 (11) 4314-3434

Asia/Pacific Rim

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9817 4550

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

<http://www.symantec.com/region/br/>
+55 (11) 3048-7515
Fax: +55 (11) 3048-7510

Colombia, Venezuela, the Caribbean, and Latin America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

<http://www.symantec.com/region/mx/>
+1 (541) 334-6054 (U.S.A.)
Fax: (541) 984-8020 (U.S.A.)

Europe, Middle East, and Africa

Symantec Customer Service Center http://www.symantec.com/region/reg_eu/
P.O. Box 5689 +353 (1) 811 8032
Dublin 15 Fax: +353 (1) 811 8033
Ireland

Automated Fax Retrieval +31 (71) 408-3782

Mexico

Symantec Mexico <http://www.symantec.com/region/mx>
Blvd Adolfo Ruiz Cortines, +52 (5) 661-6120
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

October 2000