



2012-JAN-27

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

13250 - Symantec pcAnywhere Host Services Login Remote Code Execution

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3478

BID: 51592

Description

A remote code execution vulnerability is present in some versions of Symantec pcAnywhere.

Observation

A remote code execution vulnerability is present in some versions of Symantec pcAnywhere.

The flaw is caused by improper validation of user supplied data during login and authentication with Symantec pcAnywhere host services on port 5631/TCP.

A remote unauthenticated user could execute arbitrary code by sending crafted messages to the target server in the context of the application on the affected system.

13251 - Symantec pcAnywhere Local Access File Privilege Escalation Vulnerability

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-3479

BID: 51593

Description

A vulnerability is present in some versions of Symantec pcAnywhere.

Observation

Symantec pcAnywhere product line is a remote PC control solution for Windows systems.

A vulnerability is present in some versions of Symantec pcAnywhere. The vulnerability is caused due to improper file permission set during installation of Symantec pcAnywhere. An authorized user with limited privilege could overwrite files and execute some code. Attacker could exploit the vulnerability to leverage elevated privilege.

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

13231 - Oracle Database Server Listener Oracle Net Denial Of Service

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-2012-0072

DISA IAVA: 2012-A-0014

Update Details

FASLScript is updated.

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: <https://mysupport.mcafee.com>

Multi-National Phone Support available here:

<http://www.mcafee.com/us/about/contact/index.html>

Non-US customers - Select your country from the list of Worldwide Offices.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2010 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates