Release Notes for Hot Patch 3 for Cisco IronPort AsyncOS 7.5.2 for Email Security

Revised: July 18, 2013

Contents

This document contains information about Hot Patch 3 for AsyncOS 7.5.2 for Email Security. This document includes the following sections:

Upgrade Paths

You can upgrade to release 7.5.2-203 from the following versions:

- 7.1.5-102
- 7.5.0-612
- 7.5.1-026
- 7.5.1-028
- 7.5.1-102
- 7.5.2-014
- 7.5.2-019
- 7.5.2-101

What's New

New License Agreement and Supplemental License Agreement. The IronPort End User License Agreement has been replaced and a Supplemental License Agreement has been added. Because the license agreement has changed, you may be required to accept the new agreement when you apply new feature keys after upgrading.

A copy of the new license agreement is included in the Online Help. To view it, choose **Help and Support > Online Help**, scroll down to the end of the Contents list, and click the link for the license agreement.

Resolved Issues

The following issue is resolved in this release:

Defect ID	Description
CSCzv44633	**Web Framework Authenticated Command Injection Vulnerability**
	A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an authenticated, remote attacker to execute arbitrary commands on the underlying operating system with elevated privileges.
	For more information on the vulnerability, see the Cisco security advisory at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa.

Additional Information

For additional information about Cisco IronPort AsyncOS 7.5.2 for Email Security, see the Release Notes at http://www.cisco.com/en/US/products/ps10154/prod_release_notes_list.html.

Service and Support

U.S. toll-free: 1(877) 641- 4766

International: http://cisco.com/web/ironport/contacts.html

Support Portal: http://cisco.com/web/ironport/index.html