



# Release Notes for Hot Patch 6 for Cisco IronPort AsyncOS 7.1.5 for Email Security

---

Published: June 27, 2013

## Contents

This document contains information about Hot Patch 6 for AsyncOS 7.1.5 for Email Security. This document includes the following sections:

- [Upgrade Paths, page 1](#)
- [Resolved Issues, page 2](#)
- [Additional Information, page 2](#)
- [Service and Support, page 3](#)

## Upgrade Paths

You can upgrade to release 7.1.5-106 from the following versions:

- 7.1.5-101
- 7.1.5-102
- 7.1.5-105



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

# Resolved Issues

**Table 1** *Resolved Issues in Hot Patch 6 for Cisco IronPort AsyncOS 7.1.5 for Email Security*

Defect ID	Description
<a href="#">CSCzv25573</a>	<p><b>IronPort Spam Quarantine (ISQ) Denial of Service Vulnerability</b></p> <p>A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition.</p> <p>For more information on the vulnerability, see the Cisco security advisory at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa</a>.</p>
<a href="#">CSCzv44633</a>	<p><b>Web Framework Authenticated Command Injection Vulnerability</b></p> <p>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.</p> <p>For more information on the vulnerability, see the Cisco security advisory at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa</a>.</p>
<a href="#">CSCzv63329</a>	<p><b>Management Graphical User Interface Denial of Service Vulnerability</b></p> <p>A vulnerability in the Cisco IronPort Email Security appliance that could have allowed an unauthenticated, remote attacker to cause multiple critical processes to become unresponsive, resulting in a denial of service condition.</p> <p>For more information on the vulnerability, see the Cisco security advisory at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130626-esa</a>.</p>

## Additional Information

For additional information about Cisco IronPort AsyncOS 7.1.5 for Email Security, see the Release Notes at [http://www.cisco.com/en/US/products/ps10154/prod\\_release\\_notes\\_list.html](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>

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.