

Cisco Security Advisory: IronPort Encryption Appliance / PostX and PXE Encryption Vulnerabilities

Advisory ID: [cisco-sa-20090114-ironport](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20090114-ironport.shtml>

Revision 1.0

For Public Release 2009 January 14 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

IronPort PXE Encryption is an e-mail encryption solution that is designed to secure e-mail communications without the need for a Public Key Infrastructure (PKI) or special agents on receiving systems. When an e-mail message is targeted for encryption, the PXE encryption engine on an IronPort e-mail gateway encrypts the original e-mail message as an HTML file and attaches it to a notification e-mail message that is sent to the recipient. The per-message key used to decrypt the HTML file attachment is stored on a local IronPort Encryption Appliance, PostX software installation or the Cisco Registered Envelope Service, which is a Cisco-managed software service.

PXE Encryption Privacy Vulnerabilities

The IronPort PXE Encryption solution is affected by two vulnerabilities that could allow unauthorized individuals to view the contents of secure e-mail messages. To exploit the vulnerabilities, attackers must first intercept secure e-mail messages on the network or via a compromised e-mail account.

IronPort Encryption Appliance Administration Interface Vulnerabilities

IronPort Encryption Appliance devices contain two vulnerabilities that could allow unauthorized users to gain access to the IronPort Encryption Appliance administration interface and modify other users' settings. These vulnerabilities do not affect Cisco Registered Envelope Service users.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for the vulnerabilities that are described in this advisory.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090114-ironport.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

The following IronPort Encryption Appliance/PostX versions are affected by these vulnerabilities:

- All PostX 6.2.1 versions prior to 6.2.1.1
- All PostX 6.2.2 versions prior to 6.2.2.3
- All IronPort Encryption Appliance/PostX 6.2.4 versions prior to 6.2.4.1.1
- All IronPort Encryption Appliance/PostX 6.2.5 versions
- All IronPort Encryption Appliance/PostX 6.2.6 versions
- All IronPort Encryption Appliance/PostX 6.2.7 versions prior to 6.2.7.7
- All IronPort Encryption Appliance 6.3 versions prior to 6.3.0.4
- All IronPort Encryption Appliance 6.5 versions prior to 6.5.0.2

The version of software that is running on an IronPort Encryption Appliance is located on the About page of the IronPort Encryption Appliance administration interface.

Note: Customers should contact IronPort support to determine which software fixes are applicable for their environment. Please consult the Obtaining Fixed Software section of this advisory for more information.

☐ Products Confirmed Not Vulnerable

IronPort C, M and S-Series appliances are not affected by these vulnerabilities. Although C-Series appliances can be configured to use a local IronPort Encryption Appliance for per-message key retention, the C-Series appliances are not vulnerable. The Cisco Registered Envelope Service is not vulnerable.

No other Cisco products are currently known to be affected by these vulnerabilities.

▣ Details

Note: IronPort tracks bugs using an internal system that is not available to customers. The IronPort bug tracking identifiers are provided for reference only.

PXE Encryption Privacy Vulnerabilities

Individual PXE Encryption users are vulnerable to two message privacy vulnerabilities that could allow an attacker to gain access to sensitive information. All the vulnerabilities require an attacker to first intercept a secure e-mail message as a condition for successful exploitation. Attackers can obtain secure e-mail messages by monitoring a network or a compromised user e-mail account.

The IronPort Encryption Appliance contains a logic error that could allow an attacker to obtain the unique, per-message decryption key that is used to protect the content of an intercepted secure e-mail message without user interaction. Using the decryption key, an attacker could decrypt the contents of the secure e-mail message. This vulnerability is documented in IronPort bug 8062 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0053.

By modifying the contents of intercepted secure e-mail messages or by forging a close copy of the e-mail message, it may be possible for an attacker to convince a user to view a modified secure e-mail message and then cause the exposure of the user's credentials and message content. Please see the Workarounds section for more information on mitigations available to reduce exposure to these phishing-style attacks. This vulnerability is documented in IronPort bug 8149 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0054.

IronPort Encryption Appliance Administration Interface Vulnerabilities

The administration interface of IronPort Encryption Appliance devices contains a cross-site request forgery (CSRF) vulnerability that could allow an attacker to modify a user's IronPort Encryption Appliance preferences, including their user name and personal security pass phrase, if the user is logged into the IronPort Encryption Appliance administration interface. Exploitation of the vulnerability will not allow an attacker to change a user's password. This vulnerability is documented in IronPort bug 5806 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0055.

The administration interface of IronPort Encryption Appliance devices also contains a cross-site request forgery (CSRF) vulnerability that could allow an attacker to execute a command and modify a user's IronPort Encryption Appliance preferences, including their user name and personal security pass phrase, under certain circumstances when a user logs out of the IronPort Encryption Appliance administration interface. Exploitation of the vulnerability will not allow an attacker to change a user's password. This vulnerability is documented in IronPort bug 6403 and has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-0056.

▣ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common

Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at:

<http://intellishield.cisco.com/security/alertmanager/cvss>

PXE Encryption Message Decryption Vulnerability - IronPort Bug 8062					
Calculate the environmental score of 8062					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	None	None
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

PXE Encryption Phishing Vulnerabilities - IronPort Bug 8149					
Calculate the environmental score of 8149					
CVSS Base Score - 6.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	High	None	Complete	Partial	None
CVSS Temporal Score - 5					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

IronPort Encryption Appliance CSRF Vulnerability - IronPort Bug 5806					
Calculate the environmental score of 5806					
CVSS Base Score - 5.8					
Access	Access		Confidentiality	Integrity	Availability

Vector	Complexity	Authentication	Impact	Impact	Impact
Network	Medium	None	Partial	Partial	None
CVSS Temporal Score - 4.8					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

IronPort Encryption Appliance Logout Action CSRF Vulnerability - IronPort Bug 6403					
Calculate the environmental score of 6403					
CVSS Base Score - 5.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Partial	Partial	None
CVSS Temporal Score - 4.8					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

▣ Impact

PXE Encryption Privacy Vulnerabilities

Successful exploitation of these vulnerabilities could allow an attacker to obtain user credentials and view the contents of intercepted secure e-mail messages, which could result in the disclosure of sensitive information.

IronPort Encryption Appliance Administration Interface Vulnerabilities

Successful exploitation of these vulnerabilities could allow an attacker to access user accounts on an IronPort Encryption Appliance device, which could result in the modification of user preferences.

[Top of the section](#) [Close Section](#)

▣ Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

[Top of the section](#) [Close Section](#)

▣ Workarounds

There are no workarounds for the vulnerabilities that are described in this advisory.

There are mitigations available to help prevent exploitation of the PXE Encryption phishing-style vulnerability. Phishing attacks can be greatly reduced if DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) are implemented on IronPort e-mail gateways to help ensure message integrity and source origin. Additionally, the PXE Encryption solution contains an anti-phishing Secure Pass Phrase feature to ensure that secure notification e-mail messages are valid. This feature is enabled by recipients when configuring their PXE user profile. Cisco has released a best practices document that describes several techniques to mitigate against the phishing-style attacks that is available at the following link:

<http://www.cisco.com/web/about/security/intelligence/bpiron.html>

[Top of the section](#) [Close Section](#)

☐ **Obtaining Fixed Software**

Cisco has released free software updates that address these vulnerabilities. The affected products in this advisory are directly supported by IronPort, and not via the Cisco TAC organization. Customers should contact IronPort technical support at the link below to obtain software fixes. IronPort technical support will assist customers in determining the correct fixes and installation procedures. Customers should direct all warranty questions to IronPort technical support.

Do not contact psirt@cisco.com or security-alert@cisco.com for software upgrades.

http://www.ironport.com/support/contact_support.html

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

J.B. Snyder of Brintech reported a method for obtaining PXE Encryption user credentials via a phishing-style attack to Cisco.

All other vulnerabilities were discovered by Cisco or reported by customers.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain

factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20090114-ironport.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2009-January-14	Initial public release
--------------	-----------------	------------------------

[Top of the section](#) [Close Section](#)

☐ **Cisco Security Procedures**

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

This document solved my problem.

- Yes
- No
- Just browsing

Suggestions for improvement:

(256 character limit)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)