
thunderbird security update (RHSA-2007-1083)

Original Release Date: December 27, 2007

Last Revised: December 27, 2007

Number: ASA-2007-536

Risk Level: None

Advisory Version: 1.0

Advisory Status: Final

1. Overview:

Thunderbird is a popular open source email, newsgroup and RSS client from the Mozilla Foundation.

A cross-site scripting flaw was found in the way Thunderbird handled the jar: URI scheme. It may be possible for a malicious HTML mail message to leverage this flaw, and conduct a cross-site scripting attack against a user running Thunderbird. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CVE-2007-5947](http://cve.mitre.org/cve/2007/5947) to this issue.

Several flaws were found in the way Thunderbird processed certain malformed HTML mail content. A HTML mail message containing malicious content could cause Thunderbird to crash, or potentially execute arbitrary code as the user running Thunderbird. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CVE-2007-5959](http://cve.mitre.org/cve/2007/5959) to this issue.

A race condition existed when Thunderbird set the "window.location" property when displaying HTML mail content. This flaw could allow a HTML mail message to set an arbitrary Referrer header, which may lead to a Cross-site Request Forgery (CSRF) attack against websites that rely only on the Referrer header for protection. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CVE-2007-5960](http://cve.mitre.org/cve/2007/5960) to this issue.

No Avaya system products are vulnerable, as Thunderbird is not installed by default.

More information about these vulnerabilities can be found in the security advisory issued by RedHat Linux:

- <https://rhn.redhat.com/errata/RHSA-2007-1083.html>

2. Avaya System Products with Thunderbird installed: None

3. Avaya Software-Only Products:

Avaya software-only products operate on general-purpose operating systems. Occasionally vulnerabilities may be discovered in the underlying operating system or applications that come with the operating system. These vulnerabilities often do not impact the software-only product directly but may threaten the integrity of the underlying platform.

In the case of this advisory Avaya software-only products are not affected by the vulnerability directly but the underlying Linux platform may be. Customers should determine on which Linux operating system the product was installed and then follow that vendor's guidance.

Product:	Actions:
CVLAN	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the CVLAN application. The CVLAN application does not require the software described in this advisory.
Avaya Integrated Management Suite (IMS)	Depending on the Operating System provided by customers, the affected package may be installed on the underlying Operating System supporting the IMS application. The IMS application does not require the software described in this advisory.

Recommended Actions:

In the event that the affected package is installed, Avaya recommends that customers follow recommended actions supplied by RedHat Linux.

4. Additional Information:

Additional information may also be available via the Avaya support [website](#) and through your Avaya account representative. Please contact your Avaya product support representative, or dial 1-800-242-2121, with any questions.

5. Disclaimer:

ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES

THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, INCIDENTAL, STATUTORY, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

6. Revision History:

V 1.0 - December 27, 2007 - Initial Statement issued.

Send information regarding any discovered security problems with Avaya products to either the contact noted in the product's documentation or securityalerts@avaya.com.

© 2007 Avaya Inc. All Rights Reserved. All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.