
mod_auth_kerb security update (RHSA-2006-0746)

Original Release Date: December 12, 2006

Last Revised: May 27, 2009

Number: ASA-2006-270

Risk Level: Low

Advisory Version: 2.0

Advisory Status: Final

1. Overview:

mod_auth_kerb is a 3rd party Apache HTTP Server module that provides the ability to use Kerberos authentication via HTTP.

Due to an off by one flaw that was found in mod_auth_kerb, a remote user could send a carefully constructed authentication request which may possibly crash the httpd child process handling the request. The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name [CVE-2006-5989](https://cve.mitre.org/cve/2006/5989) to this issue.

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

- <https://rhn.redhat.com/errata/RHSA-2006-0746.html>

2. Avaya System Products with mod_auth_kerb installed:

Product:	Affected Version(s):	Risk Level:	Actions:
Avaya Messaging Storage Server	MSS 3.x, 4.0	Low	Upgrade to MSS 5.0

Recommended Actions:

For all system products which use vulnerable versions of mod_auth_kerb, Avaya recommends that customers restrict local and network access to the server. This restriction should be enforced through the use of physical security, firewalls, ACLs, VPNs, and other generally-accepted networking practices until such time as an update becomes available and can be installed.

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 vendors guidance.

4. Software-Only Products:

Product:	Affected Version(s):	Risk Level:	Actions:
CVLAN	All	None	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)	All	None	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:

Avaya recommends that customers follow recommended actions supplied by RedHat Linux or remove the affected package.

5. 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.

6. 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 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, 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.

7. Revision History:

V 1.0 - December 12, 2006 - Initial Statement issued.

V 2.0 - May 27, 2009 - Changed MSS Actions and status to Final.

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

© 2006 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.