

STEEL-BELTED
RADIUS[®]

**OpenSSL Security
Advisory**

October 2006

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
(408) 745-2000
www.juniper.net

Copyright © 2006 Juniper Networks, Inc. All rights reserved. Printed in USA.

Steel-Belted Radius, Juniper Networks, and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. Raima, Raima Database Manager and Raima Object Manager are trademarks of Birdstep Technology. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Overview

Juniper Networks has identified a security problem in the OpenSSL software used by Steel-Belted Radius.

A security patch is now available for the OpenSSL vulnerability impacting Enterprise, Global Enterprise and Service Provider Editions of Steel-Belted Radius v5.3.0, v5.3.1, v5.4.0 and v5.4.1. A patch is available for the v5.3.1 and v5.4.1 releases of Steel-Belted Radius.

If you are running v5.3.0, we recommend that you upgrade to v5.3.1 and then apply the security patch. If you are running v5.4.0 we recommend that you upgrade to v5.4.1 and then apply the security patch.

Which Servers Are Affected

The problem affects SSL/TLS traffic and therefore affects:

- The Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication method
- The EAP-TLS helper
- The Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) authentication method (when client certificates or Certificate Revocation Lists are in use)

Cause of Security Problem

This vulnerability can be traced to OpenSSL software within Steel-Belted Radius. For technical details, see www.openssl.org/news/secadv_20060905.txt.

Download and Install the Appropriate Patch

Click below to download the patch appropriate for your version of Steel-Belted Radius.

Steel-Belted Radius v5.3.1

Patch number: 969531-01

- Linux Patch: Download sbr-patch-969531-01-lin.tar.gz. Unpack it. Follow the instructions in the Readme file.

- Solaris Patch: Download sbr-patch-969531-01-sol.tar.gz. Unpack it. Follow the instructions in the Readme file.
- Windows Patch: Download sbr-patch-969531-01-win.exe. Execute it. The Steel-Belted Radius server will be stopped, patched, and (if it was running) restarted.

Steel-Belted Radius v5.4.1

Patch number: 969541-01

- Linux Patch: Download sbr-patch-969541-01-lin.tar.gz. Unpack it. Follow the instructions in the Readme file within.
- Solaris Patch: Download sbr-patch-969541-01-sol.tar.gz. Unpack it. Follow the instructions in the Readme file within.
- Windows Patch: Download sbr-patch-969541-01-win.exe. Execute it. The Steel-Belted Radius server will be stopped, patched, and (if it was running) restarted.

Upgrading Steel-Belted Radius After Installing the Patch

After you install the patch, you must uninstall the patch before you upgrade Steel-Belted Radius to a newer release. For the 5.3.1 to 5.4.1 upgrade, the upgrade procedure in the *Steel-Belted Radius Getting Started* manual must be modified.

To upgrade Steel-Belted Radius from version 5.3.1 to version 5.4.1 after you install the OpenSSL patch:

1. Uninstall the 969531-01 patch.
 - On Linux or Solaris, consult the ReadMe file for the patch.
 - On Windows, use the Add/Remove Programs applet in the control panel.
2. Uninstall Steel-Belted Radius, following the directions in the *Getting Started* manual for Steel-Belted Radius v5.3.1.
3. Install Steel-Belted Radius, following the directions in the *Getting Started* manual for Steel-Belted Radius v5.4.1.
4. Install the 969541-01 patch.
 - On Linux or Solaris, consult the Readme
 - On Windows, execute the installer

When you upgrade to a release of Steel-Belted Radius later than 5.4.x, uninstall the OpenSSL patch before upgrading. You will not need to apply a new version of the patch.