RSA® Key Recovery Manager for Certificate Manager 6.9 build 566 Readme

This document includes installation information for RSA Key Recovery Manager for Certificate Manager 6.9 build 566 (Key Recovery Manager for Certificate Manager). Read this document before installing the software.

Note: You must install Certificate Manager 6.9 build 566 before you install Key Recovery Manager for Certificate Manager 6.9 build 566. For Certificate Manager installation instructions, see the *RSA Certificate Manager 6.9 build 566 Readme*.

For the complete Key Recovery Manager for Certificate Manager documentation set, go to the Key Recovery Manager for Certificate Manager page on RSA Link or contact RSA Customer Support.

Contents:

Copyright © 2018 Dell Inc. or its subsidiaries. All rights reserved.

New Features

There are no new features in this release of Key Recovery Manager for Certificate Manager.

Enhanced Functionality

This release of Key Recovery Manager for Certificate Manager is designed to include the following:

- Embedded components upgraded to the latest secure version: RSA BSAFE Micro Edition Suite 4.1.6.1. For more information, see Fixed Issues.

Package Contents

The Key Recovery Manager for Certificate Manager package for this hotfix release is designed to contain the following:

- Key Recovery Manager for Certificate Manager files:
  - `RSAKRM-CM-v6.9build566r-package.zip` (for systems running a Windows operating system)
  - `RSAKRM-CM-v6.9build566r-solaris-package.tar` (for systems running a Solaris operating system)
  - `RSAKRM-CM-v6.9build566r-linux-package.tar` (for systems running a Red Hat Enterprise Linux operating system)
  - `RSAKRM-CM-v6.9build566r-SuSE-linux-package.tar` (for systems running a SUSE Linux operating system)
- Product documentation consisting of this *Readme* document in Portable Document Format (PDF).

Note: In the event of a discrepancy, this *Readme* document takes precedence over the *Administrator's Guide* and the Help information.

Installation

Install the Full Build

To install the full build of Key Recovery Manager for Certificate Manager, use the appropriate file from this package. On systems running a:

- Windows operating system, use `RSAKRM-CM-v6.9build566r-WIN32.zip`.
- Solaris operating system, use `RSAKRM-CM-v6.9build566r-sparc-sun-solaris.tar`.
- Red Hat Linux operating system, use `RSAKRM-CM-v6.9build566r-linux.tar`.
- SUSE Linux operating system, use `RSAKRM-CM-v6.9build566r-SuSE_linux.tar`.

For full instructions on how to install Key Recovery Manager for Certificate Manager, see the *RSA Key Recovery Manager for Certificate Manager Installation Guide*.

Install the Hot Fix Files

This section describes how to install the hot fix files for this release. Instructions for the following platforms are provided:

- Windows Operating System
- Solaris or Linux Operating System.

Windows Operating System

This hotfix does not require a new installation of the product, but rather a drop-in replacement of files into the appropriate Certificate Manager directory and updating the Help.

To apply Key Recovery Manager for Certificate Manager 6.9 build 566:

1. Stop all Certificate Manager services.
2. Create a backup of the following files, where `INSTALL_DIR` is the directory path where Certificate Manager is installed:
   - `<INSTALL_DIR>\WebServer\admin-server\ca\admin-navbar.html`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\ca-ops\ca-juri-config.xuda`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\ca-ops\config-domain-logmsg.xuda`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\ca-ops\config-domain-modify.xuda`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\ca-ops\config-domain-print.xuda`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\ca-ops\config-domain-query.xuda`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\cert-ops\shared\cc-cert-view.html`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\cert-ops\shared\cert-view.html`
   - `<INSTALL_DIR>\WebServer\admin-server\ca\help\rcm-krm-help.zip`
   - `<INSTALL_DIR>\WebServer\enroll-server\get-cert.xuda`
   - `<INSTALL_DIR>\WebServer\enroll-server\get-encryption-cert-onestep.xuda`
   - `<INSTALL_DIR>\WebServer\enroll-server\request-msie-kro.xuda`

- <INSTALL_DIR>\WebServer\scripts\library.js
- <INSTALL_DIR>\WebServer\x-templates\x-construct-domain-form.xuda
- <INSTALL_DIR>\Xudad\bin\nfProvider.dll
- <INSTALL_DIR>\Xudad\bin\pkcs11Provider.dll

3. Copy RSAKRM-CM-v6.9build566r-dropin-WIN32.zip to the <INSTALL_DIR> directory.
4. Extract the files from the .zip file, ensuring the new files replace the old files.

Note: If you modified any xuda templates in your Key Recovery Manager installation, you must make those modifications again.

5. To update the Help information, in the <INSTALL_DIR>\WebServer\admin-server\ca\help directory, extract the files from rcm-krm-help.zip, ensuring the new files replace the old files.

Note: If you are upgrading from Key Recovery Manager for Certificate Manager 6.9 build551 or above, this step is not required.

6. Start all Certificate Manager services.

Solaris or Linux Operating System

This hotfix does not require a new installation of the product, but rather a drop-in replacement of files into the appropriate Certificate Manager directory and updating the Help.

To apply Key Recovery Manager for Certificate Manager 6.9 build 566:

1. Stop all Certificate Manager services.
2. Create a backup of the following files, where INSTALL_DIR is the directory path where Certificate Manager is installed:

- <INSTALL_DIR>/WebServer/admin-server/ca/admin-navbar.html
- <INSTALL_DIR>/WebServer/admin-server/ca/ca-ops/ca-juri-config.xuda
- <INSTALL_DIR>/WebServer/admin-server/ca/ca-ops/config-domain-logmsg.xuda
- <INSTALL_DIR>/WebServer/admin-server/ca/ca-ops/config-domain-modify.xuda
- <INSTALL_DIR>/WebServer/admin-server/ca/ca-ops/config-domain-print.xuda
- <INSTALL_DIR>/WebServer/admin-server/ca/ca-ops/config-domain-query.xuda
- <INSTALL_DIR>/WebServer/admin-server/ca/cert-ops/shared/cc-cert-view.html
- <INSTALL_DIR>/WebServer/admin-server/ca/cert-ops/shared/cert-view.html
- <INSTALL_DIR>/WebServer/admin-server/ca/help/rcm-krm-help.tar
- <INSTALL_DIR>/WebServer/enroll-server/get-cert.xuda
- <INSTALL_DIR>/WebServer/enroll-server/get-encryption-cert-onestep.xuda
- <INSTALL_DIR>/WebServer/enroll-server/request-msie-kro.xuda
- <INSTALL_DIR>/WebServer/scripts/library.js
- <INSTALL_DIR>/WebServer/x-templates/x-construct-domain-form.xuda
- <INSTALL_DIR>/Xudad/bin/nfProvider.so
- <INSTALL_DIR>/Xudad/bin/pkcs11Provider.so

3. Copy the appropriate .tar file to the <INSTALL_DIR> directory.
   On systems running a:
   - Solaris operating system, use
     RSAKRM-CM-v6.9build566r-dropin-sparc-sun-solaris.tar.
   - Red Hat Linux operating system, use
     RSAKRM-CM-v6.9build566r-dropin-linux.tar.
   - SUSE Linux operating system, use
     RSAKRM-CM-v6.9build566r-dropin-SuSE_linux.tar.
4. Extract the files from the .tar file, ensuring the new files replace the old files.
5. To update the Help information, in the
   <INSTALL_DIR>>/WebServer/admin-server/ca/help directory, extract the files from rcm-krm-help.tar ensuring the new files replace the old files.

   Note: If you are upgrading from Key Recovery Manager for Certificate Manager 6.9 build 551 or above, this step is not required.

6. Ensure the permissions and ownership of the extracted files match the permissions and ownership of other files in the same directories.

   For example, the files in the /WebServer directory must be readable by the user and/or group under which the server runs. If you encounter permission problems, change the ownership of the files in the <INSTALL_DIR>/WebServer directory to the user and group under which the Certificate Manager Web Server was installed.

   From the <INSTALL_DIR> directory, type:

   ```
   chown -R <install_user>:<install_group> WebServer
   ```

   Note: If you modified any xuda templates in your Key Recovery Manager installation, you must make those modifications again.

7. Start all Certificate Manager services.

Fixed Issues

The following table lists the issue fixed in this release of Key Recovery Manager for Certificate Manager:

Table 1 Fixed Issues

ID	Description
CERTMGR-4722	RSA BSAFE Micro Edition Suite 4.1.6.1 is updated to resolve the following vulnerabilities: • An integer overflow vulnerability. (CVE-2018-11054) • An Improper Clearing of Heap Memory Before Release, *Heap Inspection,* vulnerability. (CVE-2018-11055) • An Uncontrolled Resource Consumption, *Resource Exhaustion*, vulnerability when parsing ASN.1 data. (CVE-2018-11056) • A Covert Timing Channel vulnerability during RSA decryption, also known as a Bleichenbacher attack on RSA decryption. (CVE-2018-11057) • A Buffer Over-Read vulnerability when parsing ASN.1 data. (CVE-2018-11058)

For the list of issues fixed in previous releases, see the appropriate Readme documents.

Known Issues

There are no known issues for this release of Key Recovery Manager for Certificate Manager.

Support and Service

Access these locations for help with your RSA product:

- RSA Link

  RSA Link offers a knowledge base that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

- RSA Customer Support

  The RSA Customer Support site on RSA Link contains information on RSA support programs plus an extensive Content Library of product-related documents such as datasheets, guides and whitepapers.

- RSA Ready

  The RSA Ready Community is a platform for customers, partners, and RSA enthusiasts to learn about products certified to interoperate with RSA products including access to integration guides.

Before You Call Customer Support

Make sure you have direct access to the computer running your RSA product software.

Please have the following information available:

- ❑ Your RSA Customer Serial Number.
- ❑ The software version number of your RSA product.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.