Readme
RSA® Validation Manager 3.2 build201

May 15, 2015

Introduction

This document lists what's new and changed in RSA® Validation Manager 3.2 build201. It includes installation information, as well as information about the fixed issues and the known issues. Read this document before installing the software. This document contains the following sections:

For the complete RSAValidation Manager 3.2 documentation set, go to RSA SecurCare® Online at **https://knowledge.rsasecurity.com** or contact RSA Customer Support.

New Features

There are no new features in this release of RSAValidation Manager 3.2 build201

Enhanced Functionality

Support for nCipher security world with AES (SP800-131) algorithm

RSA Validation Manager 3.2 build 201 is engineered to support nCipher security world with AES (SP800-131) algorithm. RSA Validation Manager is updated with nCipher libraries v11.62.

Support for SHA-2 Hash Algorithm to generate Hash of Issuer Key and Issuer Name

In addition to SHA-1 and MD5 hash algorithms, RSA Validation Manager 3.2 build 201 is designed to add an enhancement to support SHA-256, SHA-384, and SHA-512 hash algorithms to generate Hash of Issuer Key and Issuer Name in OCSP request.

For Forward OCSP request, the default Hash algorithm is SHA-1. To change the default algorithm for Forward OCSP request,

1. Stop the RSA Validation Manager Services
2. Open the httpd.conf located at INSTALL_DIR/ValidationServer/conf
3. In the Virtual Hosts section, update HashAlgorithm directive after the ProactiveRetryTimeout directive as shown in example below.

   HashAlgorithm SHA-256

   The supported values are: SHA-1,MD5,SHA-256,SHA-384,SHA-512
4. Save and close the file
5. Start the RSA Validation Manager services

Updated Components

The following embedded components of RSA Validation Manager have been upgraded to the most recent secure versions:

- Apache HTTP Server 2.2.22 with additional security fixes upto Apache 2.2.29
- RSA BSAFE SSL-C 2.8.9.0.1
- nCipher libraries 11.62

Support for new platforms

RSA Validation Manager 3.2 build 201 can be installed on Red Hat Enterprise Linux (RHEL) 6.5 64-bit operating system, Microsoft Windows Server 2012 Enterprise Edition, and Windows Server 2012 R2 Enterprise Edition.

You must install the following libraries while installing the RHEL 6.5 operating system:

- libstdc++.so.6
- libexpat.so.0
- libuuid.so.1
- libXext.so.6
- compatible libraries

These libraries can be installed from the following packages available in the Red Hat Linux 6.5 installation CD:

- libstdc++-4.4.7-4.el6.i686.rpm
- compat-expat1-1.95.8-8.el6.i686.rpm
- libuuid-2.17.2-12.14.el6.i686.rpm
- libXext-1.3.1-2.el6.i686.rpm
- libXau-1.0.6-4.el6.i686.rpm
- libxcb-1.8.1-1.el6.i686.rpm
- libX11-1.5.0-4.el6.i686.rpm
- libXi-1.6.1-3.el6.i686.rpm
- libXtst-1.2.1-2.el6.i686.rpm

Support for new browsers

RSA Validation Manager 3.2 build 201 is engineered to support browser-based administration with the following browsers:

- Microsoft Internet Explorer 10.0 and 11.0 on Microsoft Windows Server 2008 R2 server 64-bit and Microsoft Windows Server 2012 R2 64-bit
- Firefox v31
- Firefox v17 on Red Hat Enterprise Linux 6.5

Luna SA v5.4.3-1 qualification with RSA Validation Manager

RSA Validation Manager 3.2 build 201 is qualified with Luna SA v5.4.3-1 with Client v5.4.2

Installation

You must perform all the tasks mentioned in the section “Preparing to Install” in the chapter “Installing RSA Validation Manager” of the *Installation Guide*, before Installation of Full Build.

If you want to install the full build of RSA Validation Manager 3.2 build 201, use the following files that come with this package:

- On Windows Server 2008 R2, use **RSAVM-3.2build201r-WIN32.zip**.
- On Windows Server 2012, use **RSAVM-3.2build201r-WIN32-2012.zip**
- On RedHat Linux, use **RSAVM-3.2build201r-RH_Linux.tar**.

For instructions to install Validation Manager, see the *Installation Guide.*

Note: RSA Validation Manager 3.2 build 201 does not include drop-in package. If you want to upgrade to RSA Validation Manager 3.2 build 201, refer the chapter “Upgrading RSA Validation Manager” of the *Installation Guide.*

Note: For Red Hat Enterprise Linux 6.5, in the task “Installing Red Hat Enteprise Linux 6.3 dependent package, in the section “Preparing to Install” in the chapter “Installing RSA Validation Manager” or “Upgrading RSA Validation Manager” of the *Installation Guide, Install the dependent packages detailed in section “*Support for new platforms” in this Readme. For Windows 2012, follow the same steps as mentioned for Windows 2008. If you are upgrading from Windows 2008 R2 to Windows 2012 server, create the upgrade package using **RSAVM-3.2build201r-WIN32.zip** on Windows 2008 server and complete the upgrade using **RSAVM-3.2build201r-WIN32-2012.zip** on Windows 2012 server.

Fixed Issues

This section lists the issues that have been fixed in this release and in the previous release.

Tracking Number	Description	Resolution
Fixed in build201		
VALSRV-1681	RSA Validation Manager is susceptible to the following Apache vulnerabilities: CVE-2012-3499 CVE-2013-1862 CVE-2014-0098 CVE-2014-0226 CVE-2014-0231 For information on these vulnerabilities, go to http://web.nvd.nist.gov/view/vuln/search and search by the CVE ID	This issue is resolved in RSA Validation Manager 3.2 build 201. RSA Validation Manager is built on Apache 2.2.22 and the applicable security fixes till Apache 2.2.29 are incorporated.
VALSRV-1698	RSA Validation Manager allows password caching on login page	This issue has been fixed in RSA Validation Manager 3.2 build 201. **Note:** For latest browsers, turn off autocomplete or password caching manually. Refer browser manual for detailed steps.

Tracking Number	Description	Resolution
VALSRV-1688	Prior to RSA Validation Manager 3.2 build 201, OpenSSL invalid files (openssl.exe, ssleay32.dll, libeay32.dll) are copied to Validation Manager installation directory. Validation Manager does not use those OpenSSL files.	This issue has been fixed in RSA Validation Manager 3.2 build 201.
VALSRV-1684	RSA Validation Manager SystemCA utility does not prompt for a passphrase confirmation.	This issue has been fixed in RSA Validation Manager 3.2 build 201
VALSRV-1709	RSA Validation Manager had the following vulnerabilities: CVE-2014-3566 For information on these vulnerabilities, go to http://web.nvd.nist.gov/view/vuln/search and search by the CVE ID	This issue has been fixed in RSA Validation Manager 3.2 build 201.
VALSRV-1718	RSA Validation Manager had the following vulnerabilities: CVE-2013-2566 For information on these vulnerabilities, go to http://web.nvd.nist.gov/view/vuln/search and search by the CVE ID.	This issue has been fixed in RSA Validation Manager 3.2 build 201.
VALSRV-1713	A cross-site scripting vulnerability affecting wrapPreDisplayMode and displayMode parameter could potentially be exploited by an attacker to execute arbitrary HTML and script code in RSA Validation Manager user's browser session.	This issue has been fixed in RSA Validation Manager 3.2 build 201.
VALSRV-1715	Prior to RSA Validation Manager 3.2 build 201, if Validation Manager is configured with LDAP status source type, thisUpdate attribute value is set to current time in the OCSP response.	This issue has been fixed in RSA Validation Manager 3.2 build 201. The OCSP response thisUpdate field is set to the import time of the certificate status from the ldap status source.
VALSRV-1722	Prior to RSA Validation Manager 3.2 build 201, the RSA Validation Manager stops working while processing a signed request for an uknown CA.	This issue has been fixed in RSA Validation Manager 3.2 build 201.

Support and Service

RSA SecurCare® Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Solution Gallery	**https://community.emc.com/community/conect/rsaxchange/rsa-ready?view=overview**