MICRO®
FOCUS

VisiBroker 8.5.3

Release Notes

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
http://www.microfocus.com

Revised 2016-03-14

Contents

Micro Focus VisiBroker 8.5.3 Release Notes

Installing VisiBroker

Before Installing SP3

This release updates VisiBroker 8.5. Before installing this Service Pack you must have VisiBroker 8.5 installed.

Installing SP3

To install this release:

1. Download the release archive to your VBROKERDIR folder.

2. Unpack the archive in the same folder.

3. Restart the application.

Operating Systems Supported

- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows Server 2008 (R2) (Standard & Enterprise editions)
- Microsoft Windows Server 2012 R2
- Embarcadero C++ Builder XE for Windows
- Solaris 10.x (SPARC)
- Solaris 10.x (x86 and x64)
- Solaris 11.x (SPARC)
- Solaris 11.x (x86 and x64)
- Red Hat Enterprise Linux 5.x (x86 and x64)
- Red Hat Enterprise Linux 6.x (x86 and x64)
- Red Hat Enterprise Linux 7.x (x86 and x64)
- SUSE Linux Enterprise Server 10.x (x86 and x64)
- SUSE Linux Enterprise Server 11.x (x86 and x64)
- SUSE Linux Enterprise Server 12.x (x86 and x64)
- HP UX 11i v3/11.31 on Itanium
- AIX 6.x (32 or 64 bit)
- AIX 7.1 (32 or 64 bit)
- Montavista Linux CGE V4 (x64)

For a full list of supported platforms, see http://supportline.microfocus.com/prodavail.aspx

New Features

This release provides enhancements in the following areas.

Support for MS-CAPI

VisiBroker 8.5.3 adds support for the Microsoft Cryptography API (CAPI), on Windows systems. When CAPI is fully enabled, it takes over the mechanism for some cryptographic operations, most notably generating RSA, DSA and ECDSA signatures. That means that private keys must be stored in Windows stores if CAPI is being used this way by a VisiBroker process. This is currently only supported on the client side.

You can enable CAPI support in VisiBroker C++ by setting the new `vbroker.security.useCAPI` property to `true`. CAPI support is automatically enabled in VisiBroker for Java.

The following new parameters are introduced to facilitate CAPI support:

C++

- `vbroker.security.useCAPI`
- `vbroker.security.useCAPICAs`
- `vbroker.security.useCapiCertificate`
- `vbroker.security.identityCertificates.nameMustContain`
- `vbroker.security.client.socket.allowedDigests`

Java

- `vbroker.security.mscapiAliasFix`
- `vbroker.security.identityCertificates.nameMustContain`

See the ***VisiBroker Security Guide*** for full details of CAPI implementation.

Support for TAG_ALTERNATE_IIOP_ADDRESS components in IIOP profiles

The new `vbroker.orb.tagAlternateIIOPAddress` property supports the inclusion of TAG_ALTERNATE_IIOP_ADDRESS components in IIOP profiles. See RPI 1099833 for details.

Support for Visual Studio 2013

VisiBroker 8.5.3 adds support for Microsoft Visual Studio 2013.

> **Note**
>
> Existing VisiBroker application code must be recompiled before you can use it with Microsoft Visual Studio 2013.

Support for Windows 10

VisiBroker 8.5.3 adds support for Microsoft Windows 10.

Support for TLS 1.2

VisiBroker 8.5.3 adds support for TLS 1.2 as a result of RPI 1095153.

Support for JDK 8

Support for JDK version 8 has been added for the Oracle, IBM and HP-UX JDKs.

> **Note**
>
> Note that in the default configuration IBM JDK version 8 has disabled support for some algorithms used by some older cipher suites. This means that the set of enabled cipher suites in IBM JDK version 8 is smaller than that in IBM version 7 JDK, or in the equivalent version 8 Oracle and HP JDKs.

For more information on the cipher suites enabled or supported by each of these JDKs, please visit the following sites:

Oracle Java version 8

For a list of the cipher suites supported by Oracle Java 8, see:

http://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider

HP-UX Java version 8

You can get the *Release Notes* for HP-UK Java 8 from:

https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJDKJRE80

IBM Java version 8

For a list of the cipher suites supported by IBM Java 8, see:

https://www-01.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html

IBM JDK version 8, in its default configuration, has disabled the following listed technologies. Users may still choose to configure and use them, but should be aware that in testing we have found the following to have been disabled:

- MD2 signed certificates
- RSA signed certificates with keys less than 1024 bits in length
- The SSLv3 protocol
- The RC4 stream cipher
- Diffie Hellman protocol with a key size less than 768 bits

User Documentation

New documentation released with this Service Pack is available online, from https://supportline.microfocus.com/productdoc.aspx.

Service Pack Archives do not contain the updated documentation, so the documentation accessed from within the product for these versions is the legacy documentation from the VisiBroker 8.5 GA version. Any platforms that have a new installation (such as Windows 10) will contain the new 8.5 SP3 documentation.

Resolved Issues

The resolved issues that customers have reported are listed in this section. The numbers that follow each issue are the Reported Problem Incident number followed by the Customer Incident Numbers (in parentheses). RPIs that have numbers only (and no text) are included to confirm that the RPIs have been fixed, since no further information is required.

Issues resolved in this Service Pack

This section includes issues that are resolved for the first time in this Service Pack.

- Minor documentation corrections.

  604124, 606056, 606057, 606179, 607031, 607032

- Documentation for the `PKCS12` keystore setting in the `vbroker.security.wallet.type` property has been improved.

  604513

- Some sections of the documentation dealing with product licensing referred to the now defunct location *bdn.borland.com*. These have been corrected.

  607371

- In the list of C++ properties in the ***Security Guide***, some of the SSL protocol versions were not documented for the `vbroker.security.server.socket.enabledProtocols` property. These are now documented.

  608145

- In some circumstances when using OpenSSL, the network layers could report partial completion of connection handshake, read, and write actions. These actions were not being re-tried correctly, which led to undetermined application behavior.

  The transient error states are now being handled correctly and the problems no longer occur.

  609996

- In certain very rare circumstances it was possible for a secure OpenSSL connection error to cause an attempt to send a partial data buffer without encryption. This error can no longer occur.

  610040

- When using the OpenSSL security modules some transient communication errors were not being re-tried correctly. Instead a COMM_FAILURE was being generated when none should have occurred, leading the ORB to re-marshal the whole request. This can no longer happen.

  610041

- The singleton `vbsec::SimpleLogger` is now protected against multithreaded access. See the ***Security Guide*** for details of the SimpleLogger mechanism.

  611047

- In multi-threaded applications, a race condition existed in which two or more threads could attempt to close a single OpenSSL connection object at the same time. This would result in a SIGSEGV violation.

  Thread protection code has now been added to prevent this situation from arising.

  614388

- VisiBroker code was intended to set `EstablishTrustInTarget` (within published IORs) to "`not_supported`" if the `vbroker.security.cipherList` property specified only Anonymous Diffie-Hellman cipher-suites (such as SSL_DH_anon_*). However, the faulty implementation also excluded Ephemeral DH ciphersuites (such as TLS_DHE_*).

  This feature is now fixed so that if **any** non-anonymous DH (or indeed non-DH) cipher-suites are specified, `EstablishTrustInTarget` will be set to "`supported`".

  615251

- Documentation of the properties `vbroker.orb.input.maxBuffers` and `vbroker.orb.output.maxBuffers` has been updated to describe how to disable caching.

  616137

- A new property, `vbroker.orb.allowRelativeFileIORs`, is introduced for the VisiBroker C++ ORB only.

  It defaults to `false`. If set to true, this property makes the C++ ORB accept file: scheme IORs of the form *`file:my.ior`*, and interpret them as locations relative to the current working directory.

  Note:
  This behavior matches that of the VisiBroker Java ORB, where relative locations are always allowed.

  It will become the default in a future release of the C++ ORB, so if you require the previous behavior, without relative IORs, you should modify your configuration to specify: `vbroker.orb.allowRelativeFileIORs=false`

  616290

- When loading VisiSecure into a security unaware C++ application, the property `vbroker.orb.dynamicLibs` must be used to specify the VisiSecure library name. This needed you to specify the exact full VisiSecure shared library name (including prefix and shared library suffix), which differs across operating systems and platform architectures.

  You can now enter the value `vbroker.orb.dynamicLibs=vbsec`

This loads the correct configured security provider, irrespective of the target platform. It works only the VisiBroker `lib` directory is present on the shared library load path. Note that if an absolute path needs to be specified for the VisiSecure library then the full exact library name will also still be needed.

616942

- Java code generated from IDL that contained a union with a boolean discriminant and only a `TRUE` case element could, with some compilers, emit warnings related to a function argument that would hide a member variable. These warnings are now fixed. IDL files must be reprocessed with `idl2java` for the fix to take effect.

  1084109 (2573037)

- Java code generated from IDL that contains structs with Basic Type members could emit warnings when compiled with the `javac -Xlint` option. These warnings referred to unnecessary casts in a generated 'write' method. These warnings are now fixed. IDL files must be reprocessed with `idl2java` for the fix to take effect.

  1084111 (2573037)

- The "equals" method in Java code generated from IDL sequences could, with certain compilers and warning levels, generate a warning for possible accidental assignment instead of a comparison. This warning is now fixed. IDL must be reprocessed with `idl2java` for the fix to take effect.

  1084112 (2573037)

- Introduced support for MS-CAPI. See Support for MS-CAPI for details.

  1096268 (2795399)

- VisiBroker is now certified for use with the HP complier aCC++ A.06.28.

  1098724 (2815310)

- Added support for setting TAG_ALTERNATE_IIOP_ADDRESS components into IIOP profiles. These components hold alternative host and port values which are interpreted by some ORBs as fallback addresses in the event of a client's failure to connect. VisiBroker clients do not currently interpret these properties this way. JacORB is an example of an ORB that does so. Addresses to be added are controlled by the new ORB property `vbroker.orb.tagAlternateIIOPAddress`. The alternate IIOP addresses must be specified according to the corbaloc IOR/URI host and port rules. The property takes a string value; comma-separated multiple entries are allowed. An example of this property use might look like:

  ```
  vbroker.orb.tagAlternateIIOPAddress=myhost.domain.com:54321,
  [fe80::20c:29ff:fe58:ce28]:23232,127.0.0.1:65000
  ```

  The printIOR tool has been upgraded to display TAG_ALTERNATE_IIOP_ADDRESS component contents to assist in debugging.

  1099833 (2799254)

Issues resolved in previous HotFixes

This section includes issues that were fixed in HotFixes to VisiBroker 8.5 SP2, and are now incorporated into SP3.

- If `vbroker.security.cipherList` is specified and no certificates are configured, the cipherList was ignored and all anonymous cipher suites were enabled.

  Now, when no certificates are configured, all non-anonymous cipher suites specified will be ignored; only the anonymous cipher suites specified as part of this property will remain actively available for the SSL handshake.

  605971

- The MFCryptLib/OpenSSL security provider has been fixed to ensure that a peer certificate is never trusted when there is no valid CA intermediate/root certificate provided for it.

  607261

- Fixed a leak of 400 bytes during start-up when using the OpenSSL security provider.

  607646

- Fixed a possible memory overflow affecting AIX when the OpenSSL security provider is used.

  607662

- The following cipher suites are not supported by VisiBroker's MFCryptLib/OpenSSL security provider:

  DH_DSS_WITH_DES_CBC_SHA, DH_DSS_WITH_3DES_EDE_CBC_SHA, DH_RSA_WITH_DES_CBC_SHA, DH_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DH_DSS_WITH_DES_CBC_SHA, TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA, TLS_DH_RSA_WITH_DES_CBC_SHA and TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA.

  OpenSSL itself does not support them, and so their definitions have been removed from `csstring_openssl.h`.

  610400

- When closing OpenSSL connections the underlying TCP connection was being closed before a graceful SSLShutdown exchange could take place. This changed the behavior at the peer from a graceful shutdown to an abrupt shutdown and forced the generation of a COMM_FAILURE.

  This sequence no longer occurs and the communication's disconnection sequence is now handled gracefully.

  614389

- During the running of a multi-threaded application it was possible for a thread to partially terminate a connection, then have a second thread also attempt to terminate the same session details.

Depending upon the exact timing of this race condition the effect could be either a SIGSEGV access violation at this time, or a double free and a SIGSEGV access violation at a later stage.

This can no longer occur.

614432

- The OpenSSL security layer was not correctly tracking session status and was allowing access to terminated session details. In multi-threaded applications this could cause a follow-up action to have access to a file descriptor that was by this time connected to a different client.

  This can no longer happen.

  614433

- When using the OpenSSL security provider, insufficient logging was available to diagnose OpenSSL issues encountered during the flow of data.

  The full flow level of logging is now available when "debug" level of logging is enabled. When normal error logging is enabled all OpenSSL communication error log messages are enabled, with sufficient content to determine internal OpenSSL error states if required.

  614434

- When a pair of specific OpenSSL session re-negotiation buffer underflow or overflow errors occurred, the OpenSSL Security channel could hang waiting for activity of the wrong type. The session transaction call would time out and a transaction re-marshal action would take place.

  This pause and re-marshal action no longer takes place and the original transaction completes normally.

  614436

- When the rare Solaris errors EPERM and EIO were encountered the OpenSSL security layer was not handling them correctly. The result was a COMMS_FAILURE error being raised when EPERM occurred and it should have been silently re-tried. When EIO was encountered the wrong minor code was used when generating COMMS_FAILURE. Both error states are now handled correctly.

  614438

- The segmentation fault in `CSIV2ServerReqInt::revokePrivileges()` has been fixed.

  1081290 (2529859)

- TLS 1.2 support is provided. See the ***Security Guide*** for details of the changes made.

  1095153 (2785118)

- When used on multi-processor hardware, VisiBroker was bound to execute on one processor core only. VisiBroker will now use all available processor cores.

1096219 (2794764)

- In VisiBroker for C++, `CORBA::TIMEOUT` exceptions were thrown too early even though the actual timeout had not expired.

  1096348 (2795586)

- `vbjclientorb.jar` has been fixed to include the Java classes required to support the `vbroker.ce.iiop.host` property.

  1096804 (2799874)

- The following OpenSSL cipher suite names are now available for use in the MFCryptLib/OpenSSL security provider:

  TLS_RSA_WITH_AES_128_CBC_SHA256
  TLS_RSA_WITH_AES_256_CBC_SHA256
  TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
  TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  TLS_RSA_WITH_AES_128_GCM_SHA256
  TLS_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
  TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

  These cipher suite names had previously been defined incorrectly.

  1097342 (2804783)

- Ephemeral Diffie-Hellman cipher suites are now available for use in the MFCryptLib/OpenSSL security provider. Note that Anonymous DH cipher suites remain available for use, but Elliptic Curve DH cipher suites are not yet supported.

  1097343 (2804783)

- In VisiBroker for Java, `tcpTimeout` ignored for `is_a` call.

  1099121 (2812973)

- In VisiBroker for Java, invoking the DII method caused a memory leak.

  1099467 (2820460)

- An OSAgent crash where memory allocation throws an uncaught `bad_alloc` exception has been fixed. A modification has been made to catch the exception and return `NULL`.

  1099701 (2820514)

- In a heavily multi-threaded environment, calls to SimpleLogger from different threads could cause SIGSEGV access violations.

This error no longer occurs.

1099952 (2816378)

- The SIGSEGV mentioned in the this RPI was a symptom of catastrophic memory exhaustion due to a series of major memory leaks. These have now been solved.

  1100808 (2831993)

- The fixes for RPIs 609996, 610040, 610041, 614388, 614389, 614432, 614433, 614434, 614436, 614438 and 1099952 have between them corrected how transient error conditions during the SSL handshake are handled.

  1101004 (2832629)

- Modification made to the VisiBroker SSL Connection Context to free the Timer object when GIOP Connection is closed.

  1100293 (2825962)

- Fixed a bug in thread local storage affecting 64-bit multiprocessor machines that could cause a crash under heavy load characterized by rapid repeated thread creation and finalization.

  1100805 (2829466)

Updates and SupportLine

Our Web site gives up-to-date details of contact numbers and addresses.

Further Information and Product Support

Additional technical information or advice is available from several sources.

The product support pages contain a considerable amount of additional information, such as:

- The WebSync service, where you can download fixes and documentation updates.
- The Knowledge Base, a large collection of product tips and workarounds.
- Examples and Utilities, including demos and additional product documentation.

To connect, enter https://www.microfocus.com in your browser to go to the Micro Focus home page.

Note: Some information may be available only to customers who have maintenance agreements.

If you obtained this product directly from Micro Focus, contact us as described on the Micro Focus Web site, https://www.microfocus.com. If you obtained the product from another source, such as an authorized distributor, contact them for help first. If they are unable to help, contact us.

Disclaimer

This software is provided "as is" without warranty of any kind. Micro Focus disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Micro Focus or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Micro Focus or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.