Vbrick Encoder

vbrick encoder v4.9

Release Notes

August 2020

Copyright

FCC Part 15

This equipment has been tested and found to comply with the limits for Class A digital device, pursuant to Part 15 of the FCC rules, Class A for OC-3C Interface, Class A for the SDI Interface. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numerique de la Classe A respecte toutes les exigences do reglement dur le materiel brouilleur du Canada.

CE Vbrick declares that this product conforms to the following certificate standards for electromagnetic emissions when installed according to the manufacturer's specifications: EN 55022:2006; EN 55024:1998, A1:2001, A2:2003; EN 61000-3-2:2005; EN 61000-3-3:1995, A1:2001, A2:2005.

Contents

Release Notes

Release Notes

This Vbrick Encoder software release runs on the encoding/decoding appliances and blades, as well as the Vbrick Presenter. The *Vbrick Encoder v4.9 Admin Guide* contains a detailed and complete description of all features and configuration parameters. The complete encoder documentation set is available from the Online help link in the VBAdmin management application, or at www.vbrick.com/documentation.

Updates in 4.9

Caution: While this update is not required, the 4.7 version is mandatory for all customers that use Vbrick 9000 encoders, including Presenters, with cloud-based Rev. Failure to update to at least 4.7 may introduce connectivity and control issues between the Encoder and Rev cloud.

Adopting this new version also includes all the necessary software changes from 4.7. Please plan accordingly.

For VB9000 4.8 code to work with VEMS scheduling, Force TLSv1.2 must be disabled. As noted, it is enabled by default.

Vbrick provides encoders and Presenter models within the 9000 encoder family. To date, in order to get access to the Presenter set of features, customers needed to purchase a 9000 Presenter or the Presenter Feature key to enable the features within a 9000 Encoder. In this update, Vbrick provides wide-scale availability of the Presenter features without the use for a feature license. In other words, Vbrick now provides the Presenter features to 9000s free of charge.

These features work in most 9000 encoders (please see the Admin guide for limitations) and are enabled within the user interface as a mode – either your 9000 is in encoder mode or Presenter mode. In Presenter mode you can utilize backgrounds, customized margins and borders, stream compositing based on predefined layouts, dynamic (during the presentation) input selection and changing, incorporating network streams into presentations, and other Presenter features that increase production quality.

Also included within this version is: the ability to enable communications with Rev through a proxy; and automatic re-broadcast of presenter streams on reboot.

Any customer currently utilizing Akamai SBR or MBR streaming should upgrade to this version.

Security Scans

Vbrick takes security seriously. Each release of the Encoders features are configured for the highest security and then the Encoder is thoroughly scanned by industry standard scanners. Vbrick performs these scans midway through the development process and addresses any issues found. Vbrick also scans again during the final quality pass. Vbrick endeavors not to release with any EXPLOITABLE or CRITICAL issues; however, there may be issues that are identified by the industry, added late to the test harness, and called-out in the final quality pass. While this is rare, it may happen. If it does happen, Vbrick evaluates each on a case by case basis and decides if release should be delayed or not based on the impact to customers.

Given the nature and frequency of OS update patches, Vbrick takes this decision very seriously.

Any EXPLOITABLE/CRITICAL issues found in this manner and postponed to the next release are identified below:

- Beyond Trust/Retina: Scanned August 27, 2019 with Scanner Version 6.6.1, Audits Revision 3568. The Retina EXTERNAL scan, there were 0 (zero) EXPLOITABLE findings. Additionally, there were 0 (zero) HIGH and MEDIUM findings. The Retina INTERNAL scan, there were 0 (zero) EXPLOITABLE findings except any listed below for next release. Additionally, there were 0 (zero) HIGH and MEDIUM findings except any listed below for next release.
- Nessus: Scanned August 27, 2019 with Version 8.5.2 (#199) Windows, Plug-in Set 201908262220, Policy Template Version 201908121704. Scans run: Badlock, Bash ShellShock, Basic Network, DROWN, ExternalPCI, InternalPCI, SpectreMeltdown, WannaCry. There were 0 (zero) CRITICAL findings except any listed below for next release. Additionally, there were 0 (zero) HIGH and MEDIUM findings except any listed below for next release.
- Late failing issues identified to be resolved in next release: No identified issues.
- Miscellaneous notes, False Positives or Issues that will not be addressed: Nessus External PCI highlighted CVE-1999-0524 as a high, when it's CVSSv2 Severity is a Low.

Urgent11 Fix Updates

Recently, there are public reports of vulnerabilities with respect to various versions of the WindRiver vxWorks (Real-time Operating System, ROS). These vulnerabilities are collectively called **Urgent11**.

Additional information can be found at Tenable (the provider of security scanning solutions) at https://www.tenable.com/blog/critical-vulnerabilities-dubbed-urgent11-place-devices-running-vxworks-at-risk-of-rce-attacks. The Vbrick 9000 family of encoders utilizes affected versions.

The Vbrick engineering team worked directly with WindRiver and has addressed the impacted Urgent11 issues by applying their patch or through software mitigation. Vbrick has applied solutions to each of the following:

- **CVE-2019-12256 9.8** Stack overflow in the parsing of IPv4 packets' IP options. **Note: N/A for Vbrick**.
- **CVE-2019-12257 8.8** DHCP Client Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc. **Implemented**.
- **CVE-2019-12255 9.8** TCP Urgent Pointer = 0 leads to integer underflow. **Implemented**.
- **CVE-2019-12260 9.8** TCP Urgent Pointer state confusion caused by malformed TCP AO option. **Note: N/A for Vbrick**.
- **CVE-2019-12261 8.8** TCP Urgent Pointer state confusion during connect() to a remote host. **Note: N/A for Vbrick**.
- **CVE-2019-12263 8.1** TCP Urgent Pointer state confusion due to race condition. **Implemented**.
- **CVE-2019-12258 7.5** DoS of TCP connection via malformed TCP options. **Implemented**.
- **CVE-2019-12259 6.3** DoS via NULL dereference in IGMP parsing. **Implemented**.

- **CVE-2019-12262 7.1** Handling of unsolicited Reverse ARP replies (Logical Flaw). **Implemented**.
- **CVE-2019-12264 7.1** Logical flaw in IPv4 assignment by the ipdhcpc DHCP client. **Implemented**.
- **CVE-2019-12265 5.4** IGMP Information leak via IGMPv3 specific membership report. **Implemented**.

Scanners that report Urgent11 issues through comparisons of vxWorks versions will falsely report Urgent11 vulnerabilities.

New Features & Issues Addressed

This release is provides a number of features, fixes, and coverage for the Urgent11 vulnerabilities. Please review the list below.

Feature	Description
Security Enhancements	The following were added/fixed in this release: • Addressed Urgent11 vulnerabilities (see expanded discussion in scan section) • Expanded use of Ephemeral keys • Fixed penetration issues (Predictable Session ID, UI Auto-complete disabled for password forms, "Secure" session cookies, HTTP security header settings) • Visible passwords on Log Page. Removed SSH Weak MAC algorithms. • Removed CBC SSH ciphers • Fixed handshake re-negotiation issues
CloudFront	Verified the encoders ability to utilize AWS Elemental MediaLive for customers with AWS accounts. See: FFMPET RTMP to AWS Elemental MediaLive to AWS Elemental MediaPackage Worflow Example for tested workflow.
Closed Captioning Improvements	Changed closed caption metadata generation to improve playback on iOS devices. To take full advantage of this improvement set **Closed Caption AUs Per RTP Packet** to "2" on the **Encoder Configuration > Global** page of VBAdmin. See: Encoder Configuration > Global
Performance or Issue Improvements	The following were added/fixed in this release: • Modification to close down specific TCP connections (when Rev controls the encoder) more effectively • Fixed (rare) issue with memory control and CURL
(DHCP Offer) Client ID Parameter Support	Added support for optional Client Identifier parameter in DHCP Offer response.
Miscellaneous	Miscellaneous updates this release: • New look and feel with updated logos.

System Description

Available Encoder Models

Vbrick Encoders include enterprise and blade models with a variety of interfaces and configurations. Contact Vbrick or your certified Vbrick reseller for more information.

Application Compatibility

The encoder is compatible with the applications shown in the table below. *Use the software versions shown or higher*

Table 1. Encoder Compatibility †

Application	Vendor	Notes
VEMS 5.x	Vbrick	Supports viewing and recording of live streams only.
VEMS 6.x	Vbrick	Supports viewing and recording of live streams. Supports scheduling for the first channel on any model.
DME 2.0	Vbrick	Fully compatible.
StreamPlayer 5.2	Vbrick	Fully compatible.
VBDirectory 5.3	Vbrick	Fully compatible.
QuickTime 7.x	Apple	If not installed, download from Apple website. If you have streaming problems with QuickTime 7.6, go to QuickTime Preferences > Advanced > Video > DirectX and uncheck **Enable Direct3D video acceleration**.
VLC 2.x	VideoLAN	VLC is not fully tested or supported by Vbrick.

† The encoder is fully compatible with the application versions shown or higher.

Operating Guidelines

Operating Notes

- Some Video and Audio configuration changes can cause a 15-20 second interruption on all channels.
- Problems may occur when installing VBDownload on Windows 7 machines if UAC (User Access Control) is enabled. If you experience problems with VBDownload, either right-click on the shortcut and select **Run as Administrator**, or disable UAC prior to installation.

Playing 720p and 1080p Streams

In order to play 720p or 1080p streams on a PC you need an adequately powered hardware platform and an efficient player. Although Vbrick can make no specific guarantees as to the performance of a particular hardware configuration, the guidelines in the table below are strongly recommended.

Table 2. Guidelines for Playing 720p and 1080p Streams

Minimum Processor	Intel Core2 (Dual- or Quad-core) processor with 2.0 GHz minimum clock speed (or AMD equivalent).
Recommended Processor	Intel i3, i5 or i7 family (Dual- or Quad-core) processor with 2.0 GHz minimum clock speed (or AMD equivalent).
Graphics Card	Nvidia/ATI graphics card. Newer model with discrete (not integrated) design.
Operating System	64 bit operating system recommended.

Quad Model Configuration Rules

These rules apply to quad models only and are enforced by the VBAdmin management program.

Table 3. Quad Model Support and Restrictions

Supported Configurations	2 channels @ 1080p60 configured as follows: • Slot1 / Ch1 (no Slot1 / Ch2) • Slot 2/Ch1 (no Slot2 / Ch2) • 4 Channels @1080i/60†

† On a per slot basis, if the input is 1080i60/50 and both channels are enabled, both channels must have a Target Frame Rate equal to or less than 30 frames/sec.

Multiple Bit Rate Configuration Rules

There are certain configuration constraints that are automatically enforced when using multiple bit rate encoding. The following errors may occur in certain configurations:

- Media processor first stage bandwidth exceeded. See documentation.
- Total encoder output is too high. Enable fewer rates, or use lower resolution or frame rates.

When encountering these errors, you may cut back on one or more of the following to obtain a legal configuration:

- Number of inputs
- Format of inputs
- Number of rates
- Resolutions
- Frame rates

Avoiding Overload Conditions

The encoder has numerous configuration options and some user configurations can overload the host processor. This is indicated by the **Current Operational Mode** reporting an "overload" on the Monitor > System page. (You can also check that the CPU monitor on the Dashboard does not exceed 90%.) Transport Stream and TCP clients are more CPU intensive than RTP and UDP clients. CPU loading can be decreased by reducing some or all of the following: Target Bit Rate, number of streams, transmitters, and clients. Another option is to increase the **Max Packet Size** on the Encoder Configuration > Global page but proceed with caution as this may cause issues in some IP networks and with some players.

KLV Metadata Support

KLV metadata is supported on the serial port(s) and on the network port. If you are using the serial ports on a device with multiple channels, only the first two channels support KLV metadata in the stream: Channel 1 uses COM2 and Channel 2 uses COM1. If you are receiving KLV or CoT into the encoder over the network, only one metadata feed can come in this way, although a second KLV or CoT feed can come in over the serial port. For more about KLV see the "KLV Metadata" chapter in the encoder admin guide.

HDCP Support

High Bandwidth Digital Content Protection (HDCP) is a form of encrypted, digital copyright protection developed and licensed by Intel that prevents copying of digital audio and video content moving over DVI or HDMI interfaces. *The encoder is designed to enforce digital copyright protection and will not encode HDCP-protected data.* This means if the video source from a DVD player, for example, is HDCP-protected, it will not be encoded by the encoder and you will typically get a **Video Input Problem** message on the Monitor > Encoder Status > Video Input page. This is not an error; this is the expected behavior.

The High Definition (HD) inputs on the encoder include HDMI, SDI, and component. Of these, only HDMI supports HDCP. In most cases video cameras with HDMI outputs will work with the encoder because they do not generally implement HDCP. Most DVD players on the other hand will not work because they do implement HDCP. To avoid HDCP conflicts with HD input, use a video camera for input to the HDMI port whenever possible; use the component port to connect a DVD player or similar device. It is also possible that video input errors have nothing to do with HDCP. For example conflicts may occur when multiple inputs from the same DVD player are connected to the encoder. If you get unexpected results—for example no video, or video but no audio—it is always a good idea to unplug all of the unused inputs.

Software Upgrade

Vbrick will periodically release new versions of the encoder's software when new features and functions are available. To upgrade your software when a new version of code is available see the "Software Upgrade" topic in the encoder *Getting Started Guide*.

Caveats

This section addresses known issues in this release, most of which have an easy workaround. For more information about any item, or help with an issue not listed here, contact your reseller or Vbrick Support Services. The caveats are grouped as follows:

- 9000 Encoder/Decoder
- Media Players
- Browsers

9000 Encoder/Decoder

- Translating 1080p60 streams down to 24 FPS streams may introduce slight stuttering. To avoid this, it is recommended that you use 30 FPS.
- For RTMP to inter-operate with the DMEs running version 3.2 or earlier, you must change the default setting of **RTMP ID** from **Vbrick** to **FMLE** on the **Transmitters** page. The DME 3.3 (and beyond) will accept either Vbrick or FMLE as the RTMP ID setting.

- Closed Caption AUs per RTP packet values over 15 can garble Closed Captioning in RTMP streams. (2135)
- RTMP DVR with Closed Captioning causes the AMS server to drop packets. (2116)
- 3.x or higher builds cannot be loaded on units that are running 1.0.x software. The workaround is to download 2.0.x first and allow it to come up then download 3.x.x. VBdownload will warn if this download is attempted. If you load 3.x over 1.0.x the encoder will become inoperable and will have to be returned to Vbrick.
- Encoders with **Board Assembly Number** 6106-0000-0101 or lower can play a maximum of one rate above SD resolutions per channel. To identify the **Board Assembly Number**, open VBAdmin and go to Monitor > System > Manufacturing Information.
- If you have a Transport Stream configured with closed captions at 60 fps, pop-up style closed captions will not play properly in VEMS Mystro (or in StreamPlayer if **Overlay CC on Video** is enabled). To work around this issue use an RTP stream. (1855)
- VBDirectory cannot connect to VBAdmin if the **External VBAdmin** parameter is set to **HTTPS Only**. (1364)
- The encoder does not detect a Video Format from some video cameras (e.g. a Sony HDR-CX160) that have an HDMI "Auto" mode (that tries to determine the best format for the attached output device). To work around this issue, do not use “auto” mode. Set the camera to the desired format (e.g. 1080p60). (974)
- For optimum performance when using an AmiNET130 Transport Stream, **Max Packet Size** (on the Encoder Configuration > Global page) should not exceed 1480. Packet Size = 1316 is optimal.
- Because of a bug in the Darwin server, the first AutoUnicast may fail (with no video) when pushing a stream to a Darwin server via UDP (Auto Unicast via TCP is not affected). The connection to the Darwin server will appear successful and the failure will become apparent only when an end user connects to the Darwin and receives only audio. To workaround this issue, create a second Transmitter with a different publishing point (Auto Unicast Dest Pub Point Name) on the server. (2898)
- If you have any IP address configured in the system with an address outside your local subnet, and did not configure a gateway (on the System Configuration > Network page), then that IP will default to the loopback address (127.0.0.1) after a save and reboot. To work around this issue always configure a gateway. (627)
- If using RTMP or AutoUnicast TCP transmitters, leave **Max Packet Size** at the default value (1452) or the transmitter session will experience problems. (616)
- Most counters rollover at 4GB (4,294,967,296). (880)
- For security reasons, encryption keys cannot be restored via a saved XML file. If you are restoring a configuration with encryption, use the following procedure:
  a. Enter the encryption keys manually; they must be entered in the same order and using the same **Key ID** and **Key Value** as the original configuration.
  b. After entering the encryption keys manually, restore the saved XML configuration.
- When a 7000 Series encoder is running at 1080i or 1080p using the "Best Quality" template, the audio and video from a 9000 Series decoder will be out of sync and the Jitter Queue Minimum Depth and Jitter Queue Average Depth will be negative numbers on the Monitor > Decoder Status > Receivers/Video/Audio page. To work around this issue, use a different template or set the Jitter Queue Time (on the Decoder Configuration > Receivers page) to a higher value. The Jitter Queue values should return to zero or higher and the audio and video will be in sync. (1457)

- EnDec models cannot decode an audio stream with a 44.1k sampling frequency if the encoder is configured for analog audio. In this case audio will be suppressed on the decoder but video will still play. (1222)
- A low Jitter Queue Time on the decoder causes garbled audio or out-of-sync audio and video. See Jitter Queue description in the Decoder Configuration > Receivers topic in Admin Guide. (1368)
- EnDec models may experience a streaming outage of about 45s that can cause connections to drop and have to be reestablished. (2187)
- Under heavy streaming and recording loads an Archiver using external USB storage may stop recording. If this happens the unit must be rebooted. (2105)
- A Presenter encoder will stop streaming if Shutdown on Video Input Problem is enabled and slot1/channel 1 Video is not connected. (2346)
- Audio mapping in a Presenter encoder does not transition seamlessly if audio rates are configured with different values. This means when switching audio sources during a presentation, the stream may need to be reset after the change. This is a known issue. The encoder interface will display an error message if this will occur.
- Changing audio channels during a presentation is not supported for streams with encryption. (ENC-48)
- Audio stream from digital input does not play when the video is disabled. (2345)
- HDMI sources that are supplied without digital audio need the digital audio disabled with the user interface.
- When using a VGA source on Component input the video may look pink and not be aligned for the following input formats: 720x480, 1280x720, 1920x1080. (2275)
- Inserted CC does not work on Presenter encoder. (2326)
- Presenter Mode access without a password will not work if operator login name changed. Workaround: Do not change the operator user name. (2084)
- Streams may suffer video quality degradation under the following circumstances: Video input format is 60 or 50 FPS, closed captioning is enabled and encoder frame rate is 15 FPS or less. (2100)
- Some configuration error messages may be hidden by VBAdmin when **Video Format Auto-Detec**t is enabled. If clicking Apply fails on the Encoder Configuration > Video Input page and you do not see an error message, try disabling **Video Format Auto-Detect** temporarily to see the message. (ENC-56)
- Errors may not always be clear when using the **Revert** button on the Presenter Mode user interface. If unclear, change the setting directly instead of using **Revert**. (ENC-25)

Media Players

The following caveats refer to issues with Vbrick StreamPlayer, Apple QuickTime, or VideoLan VLC Media Player.

StreamPlayer

- Streamplayer may experience corrupted video and audio if multicast and unicast streams from the same source are using the same IP port number. (1281)
- Audio-only encoder streams are not supported by VEMS and may result in unpredictable behavior. For example they will not play in StreamPlayer, they cannot be added to a Wowza server, etc. (9075)

QuickTime

- RTSP/RTP streams with video only (no audio) will not play in QuickTime. To work around this issue use another player, for example the Vbrick player or VLC. (446)
- To play encoder streams on Windows PCs with Apple QuickTime, version 7.0 or higher must be installed.
- To use QuickTime Player for live RTP streams, go to Edit > Preferences > go to QuickTime Preferences > Advanced > Video > DirectX and uncheck **Enable Direct3D video acceleration**.
- QuickTime may go slightly out of sync after 24 hours or more of continuous operation. If this happens, restart the QuickTime player. (1509)
- QuickTime does not fully decode SBR audio streams. This is a QuickTime bug.
- Be aware that QuickTime performance is highly dependent on the power of the graphics card installed on your computer especially when playing high resolution and high bit rate streams. (3104)
- When streaming to QuickTime players, a **Max Packet Size** less than 1000 may cause audio dropouts. (1010)

VLC

- Changing the Closed Caption Insertion Display Row value doesn't move the CC on the VLC player. (1732)
- VLC may experience corrupted video and audio if multicast and unicast streams are using the same IP port number. This can occur even if the streams originate from different sources. (1020, 1281)
- When using the "Custom" **Mode** (on the Encoder Configuration > Streams page) audio will not play in **VLC if PTS-PCR Gap** is set to 2000 or higher. To work around this issue, set value below 2000 and the audio will play. (333)
- VLC player will not play audio for streams configured with "Dual" Audio Source. (483)
- RTP Metering distorts video on VLC player. (639)
- VLC will play an audio-only stream via a transmitter--not via a server. (1831)
- VLC has issues playing a RTSP Transport Stream with Closed Captioning enabled if the stream is at 30FPS. (1872)

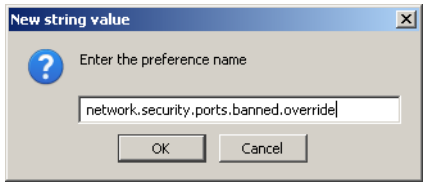
Multi-Format Set Top Box

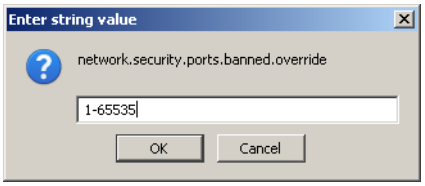
- Multi-format Set Top Box can't play video resolution 1600x1200.

Browsers

Firefox

- After changing the **Secure VBAdmin Server Port** (on the System Configuration > Advanced Configurations > Security page) from the default (443) the browser will be unable to connect to VBAdmin via HTTPS. To work around this issue:
  a. Open Firefox, type **about:config** in the address bar, and ignore any warning.
  b. Right-click in any blank area of the page and select New > String.
  c. Enter string name **network.security.ports.banned.override**, string value **1-65535**, and click OK. (2738)


New string value
Enter the preference name
network.security.ports.banned.override
OK
Cancel


Enter string value
network.security.ports.banned.override
1-65535
OK
Cancel