



CRS Build 12.0/VIP Build 4.0 Release Notes

These notes document the new features and bug fixes incorporated into the CRS Build 12.0 and VIP Build 4.0 software releases. Trouble Ticket Request (TTR) numbers have been provided to reference formally documented problems that have been resolved by this build. The following TTRs are listed numerically in two categories: Software enhancements and bug fixes.

SOFTWARE ENHANCEMENTS - CRS

1. **TTR 952: Message Association Table Replacement Processing Is Inconsistent** – The Message Association Table (MAT) Replacement capability allows CRS users to define a single Message Type to replace one or more other Message Types. For example, the ADR Message Type must replace all other HazCollect Non-Weather Emergency Messages (NWEMs). The MAT replacement function is used to define which NWEMs the ADR will replace, assuming their Listening Area Codes are identical. However, the MAT replacement capability will not actually replace a watch/warning message until it has broadcast at least once. Therefore, if three or more warnings are received in immediate succession followed immediately by a message that should replace the warnings, the replacement function will not immediately take place for all the messages. Prior to CRS Build 12.0, CRS would make a maximum of two passes to see if could replace any of the warnings. If not all the warnings had broadcast, it would make a second pass, but no more. Therefore, in most cases it would only replace the two warnings already broadcast. The remaining warnings that had not broadcast during the first two passes would continue to broadcast and would not be replaced.

CRS Build 12.0 has been modified to continue to check to see if it can replace all potential warnings (once they have broadcast) until all replacements have been made or until 60 minutes have elapsed, whichever comes first.

2. **TTR 955: Alert Monitor Trigger** – The CRS GUI has a screen saver that will cause the Main Processor displays to become blank after a period of time. Prior to CRS Build 12.0, the display would resume only after the operator initiated a keystroke. The operator would have to periodically activate the display to check the status of the Alert Monitor.

CRS Build 12.0 has been modified so that when the screen saver is engaged on the master console and a new message comes into the Alert Monitor, the screen saver is overridden and the Alert Monitor is displayed on the master console.

3. **TTR 960: Reduce SNQM Logging Output** – The Secure Network Queue Manager (SNQM) provides the mechanism by which all message communication between processes running in the CRS will take place. Prior to CRS Build 12.0, SNQM displayed several incoherent logs that could cause hundreds of file seeks/writes per second, depending on the current CRS processing load. This could CRS instability during the most busy CRS times, i.e. during severe weather. Also, the SNQM logging level logic ignored the value set in the configuration file. The SNQM software hard coded the logging level to include the most verbose level of logging (debug).

CRS Build 12.0 has been modified to set the default SNQM log level to 0, so that only fatal errors are routinely logged. This will alleviate significant stress on CRS, especially during peak message processing times. Additionally, the logging mechanism has been changed to increase the SNQM error log level (by manually editing the configuration file) without restarting CRS to allow for additional debugging information to better analyze system problems. Additional log messages have been defined to provide more descriptive information related to SNQM transactions. Lastly, appropriate labels have been added to the log messages that correspond to the type of warning, i.e. Fatal, Error, Message, Debug. **The reduction of SNQM logging messages speeds up CRS processing. However, the increased throughput results in SNQM resource errors when trying to shadow certain database transactions to the other MP and the FEPs. Therefore, until this problem can be alleviated in a future software build, the SNQM logging level will be returned to the debug setting.**

4. **TTR 962: Add CRS Performance Metrics** – CRS Build 12.0 collects CRS stop/start statistics from each site. New software collects the data, and once weekly it is collected on the NOAA4 server where it can be analyzed off-line. Additional performance metrics will be added over time. These data will aid in diagnosing site problems. **Because of questions concerning the impact of this function on network loading and how to ensure proper recovery of data following download failures, the generation of the data logs will be turned off until the implementation of a future software build.**
5. **TTR 963: Default Setting For The Message Type Disposition Parameter** – The Message Type Disposition parameter indicates whether the Weather Message is to be saved or deleted following its final broadcast. It can be saved permanently in the database or deleted. Normally, Weather Messages should be deleted after they have expired to avoid cluttering up the database. Therefore, it is recommended that the Message Type Disposition parameter be set to “Delete”. However, prior to CRS Build 12.0, the default setting for the Message Type Disposition parameter was “Save”. Therefore, if operators were not careful, they could unknowingly have messages saved after they expired and clutter up the database.

CRS Build 12.0 has been modified to change the default setting of the Message Type Disposition parameter to “Delete” to decrease the likelihood of accidentally saving unwanted old, expired messages in the database.

6. **TTR 969: IMR Replaced Messages Purged From Database When Replacement Occur**
– Prior to CRS Build 12.0, messages replaced by the Identical Message Replace (IMR) rule (same Message Type, identical LACs, identical MRD if present), such as an hourly observation replacing the previous hour's observation, would stay in the CRS database until the message's original expiration time. This would add messages unnecessarily to the CRS database and make navigating through those messages more complicated and time consuming. Perhaps more importantly, multiple expired messages would be purged simultaneously because they have the same expiration time, as would be the case for a max 13 transmitter site generating an hourly observation message for each transmitter.. This situation can cause CRS resource problems that force CRS to stop and restart.

CRS Build 12.0 has been modified to purge messages from the database when the IMR replacement takes place. This change will cause the purging to occur more gradually as each new message is processed and the old one replaced.

7. **TTR 970: CRS Security Scan Updates** – Routine security patch vulnerabilities found during the quarterly scan process have been removed.
8. **TTR 971: Add MMI Option To Clear The Logging Buffer** – The Message Monitor display (MMI) contains system-level (non-CRS related) messages that may or may not be of interest to the operator. Prior to CRS Build 12.0, the information in the display was cleared only when the operating system was stopped and rebooted. Therefore, if a site had not rebooted the Master MP in some time, the MMI could have become quite lengthy and taken a long time to display when CRS first came up. Also, the MMI data comes directly from the device. Therefore, the data can not be filtered before being sent to the MMI.

CRS Build 12.0 has been modified to clear the logging buffer so the MMI is not as lengthy. To clear the display, the user will right click on the MMI display and then select "clear".

9. **TTR 979: DST Extension** – CRS uses UTC for all message processing. Only sites that broadcast the internally generated time message need to use local time. Effective in 2007, Daylight Savings Time (DST) begins the second Sunday in March and ends the first Sunday in November. There is no patch available to make these changes in the UnixWare Operating Systems being run on the CRS MPs and FEPs.

CRS Build 12.0 has been modified to change the profile build script, which modifies the global user profile (/etc/profile). The change modifies the "TZ" environment variable so it contains the correct start/end date for DST.

10. **TTR 980: FEP Software That Generates Time Announcement Message Ignores DST Extension's New Setting (TTR 979)** - The correction described in TTR 979 allows the system time and the MP GUI display to reflect the correct local DST starting on the second Sunday in March. However, CRS is started by the inittab daemon which does not run a profile. Therefore, the CRS software on the FEP does not pick up the change described in

TTR 979, and the time announcement message does not reflect DST until the pre-2007 date.

CRS Build 12 moves the new DST string from `/etc/profile` to `/etc/TIMEZONE` on the FEPs. The new install procedure checks the MP for the correct timezone (since we can not depend on the FEP value in `/etc/TIMEZONE`) and then copies that value along with the new DST start and end parameters into the `/etc/TIMEZONE` on each FEP.

SOFTWARE ENHANCEMENTS – VIP

1. **TTR 964: Change Time Synchronization To Include VIP** – Time is synchronized from the Master MP to the Shadow MP and the FEPs twice per day. One of these twice-daily synchronizations includes a time update from one of the AWIPS processors. Prior to VIP Build 4.0, the VIP time was not synchronized with the other CRS processors. This could have lead to a gradual clock drift over time.

VIP Build 4.0 adds a once per day cron job that requests a time update from the Master MP.

2. **TTR 967: VIP Security Scan Changes** – VIP Build 3.2 includes the Fedora Legacy security patches to Red Hat Linux 7.3.
3. **TTR 973: Spanish Special Characters Are Replaced With Blanks** – VIP version 3.2 did not update a SpeechWorks system library. This caused Spanish special characters to be replaced with blanks. The problem was previously corrected at the few sites using Spanish.

VIP Build 4.0 updates the SpeechWorks system library so that Spanish special characters are handled properly by the VIP.

4. **TTR 974: Turn Off VIP Password Aging For CRS And Root Users** – Prior to VIP Build 4.0, the VIP had root and crs user password aging activated. This meant users would be forced to change VIP crs and root passwords every 90 days. Users may not have realized their password had expired until they were attempting to perform a time-critical function for which crs or root privileges were required. Therefore, a TIP was distributed directing sites to manually deactivate crs and root password aging on the VIP. Also, the password aging was deactivated in VIP version 3.2.1, which available for downloading from the NOAA4 server.

VIP Build 4.0 has been modified to turn off VIP crs and root user password aging.

5. **TTR 978: Add RAH and VEF To And Remove HNX From Spanish License Table** – The VIP contains a table of site identifiers of those offices that are permitted to use the VIP Spanish voice. Raleigh, NC (RAH) and Las Vegas, NV (VEF) had requested licenses to generate Spanish messages. Only one Spanish license is available, so Hanford, CA (HNX) agreed to give up their license. The table was modified to reflect these changes and installed at RAH, VEF, and HNX only.

VIP Build 4.0 has been modified to include RAH and VEF in the Spanish license table and to remove HNX.

BUG FIXES – CRS

1. **TTR 940: Add Transmitter Conflict With Spanish Trailer Block** – CRS Build 12.0 corrects two problems relationship between the add transmitter (addxmt) and crs_site utilities:

- a. Prior to CRS Build 12.0 running crs_site to load a database ASCII file into the CRS database from the addxmt utility automatically used an option which forced crs_site to skip various checks. This forced the line pointer to not be incremented until crs_site began to search for the next block. If within the current block, a “:” character was encountered, crs_site thought it found a new block and stopped the search. But since it was not really a new block, crs_site would return an error stating “Key does not compare to BLOCK – Unknown keyword on line <>”. This problem would not occur if the user exited addxmt and then ran crs_site from the XCRS_SITE window.

CRS Build 12.0 modifies crs_site to check for “:BLOCK” for a new block rather than just the “:”. This guarantees that crs_site has located a new block section unless the specific string “:BLOCK” is included within a block in the database ASCII file.

- b. Prior to CRS Build 12.0, the addxmt utility adds a general suite for the new transmitter that includes the Message Type STATIONID. This is so the new transmitter will broadcast a station identifier message when CRS initially comes up after the transmitter has been added. If the STATIONID Message Type does not already exist in Block 10 of the database ASCII file, crs_site will fail.

CRS Build 12.0 modifies crs_site to search Block 10 for the STATIONID Message Type. If it is not found, it will be added, and the designation number with the designation number set to the proper value for a station identification message.

2. **TTR 946: Unable To Clear Alert Monitor When Run As Root Procedure** – Sometimes the Alert Monitor may have so many messages that it is too time consuming to acknowledge each one to clear them. In such cases, it is preferable to use the procedure in Appendix H of the System Administration Manual. This procedure instructs the user to manually stop the Alert Monitor process and then use the DBBuild utility to destroy and rebuild the Error Table. Prior to Build 12.0, sometimes when the procedure was run as root user, it was not possible to restart the Alert Monitor because the owner of the Error Table was changed to root:sys.

CRS Build 12.0 changes the DBBuild utility to change the ownership of the newly created

Error Table to crs:crs. If the user tries to run DBBuild as root user, an error message will be returned and it will not run.

3. **TTR947: CRS Database Restore Failure** – If during CRS initialization there was a problem with the database and the database validation and verification (db_vv) process failed, CRS would terminate and attempt to re-start. Prior to CRS Build 12.0, there was a 30 – 60 second window of opportunity during this process where CRS was not completely down, but a user could have initiated a database recovery either with crs_site from the database ASCII file or with the Database Restore capability. This problem existed because crs_site and the database restore software do not check the status of the system before modifying the CRS database.

CRS Build 12.0 modifies the crs_site and database restore software to check /etc/inittab for an indication of a respawn, which signifies that CRS was not shutdown in an orderly fashion. When they find the respawn, crs_site and database restore will terminate.

4. **TTR 956: CRS Message Input Processing Does Not Check For Duplicate LACs As A Result Of Overlapping Zones** - Prior to CRS Build 12.0, messages received by CRS slated for SAME encoding using zone codes rather than county codes were susceptible to the following problem: If multiple listening zones mapped to the same counties, the message handling software made no attempt to eliminate the duplicates appearing in the SAME coding. This caused no problems for the NWR receivers, but could have artificially caused the message to reach the maximum number of county codes (31) allowable in the SAME coding.

CRS Build 12.0 modifies the message handling software to eliminate duplicate listening area codes in the SAME coding.

5. **TTR 959: Error With Creating CRS AWIPS Node Configuration File** – The AWIPS authorization file is used for communications with AWIPS processors. It contains the IP addresses for all AWIPS processors that CRS may communicate with for time updates and routine AWIPS interface checks. Eleven sites contain IP addresses that are off by 130 from the standard addresses. CRS Build 11.0 mistakenly left out the logic that computes the offset addresses necessary for the 11 sites. Those sites manually edited their AWIPS authorization files to correct the problem.

CRS Build 12.0 corrects the post install script to correctly set the IP addresses of the eleven offset sites in the AWIPS authorization file.

6. **TTR 961: Modify ALL Memory Manipulation Function To Function-N** – CRS Build 11.0 included a fix to TTR 950, which intermittently caused the database message handler (db_mh) to fail. The problem occurred when memory was deallocated and returned to the system if the necessary address needed to deallocate was overwritten due to a buffer overflow. The fix was to modify db_mh string functions to guarantee that only the allowed

size of data is transferred from variable to variable, thereby reducing the risk of db_mh buffer overflows.

CRS Build 12.0 extends the changes done in db_mh to all such string functions in all parts of the CRS code.

7. **TTR 966: Time Synchronization With AWIPS** – Two problems were fixed:

a. CRS contains a perl script that checks for the AWIPS processors' echo port as part of the AWIPS connectivity check at initialization and every 30 minutes thereafter. When the DX OS was updated to RHEL4, the perl script was no longer compatible with the DX's, so the echo port check always failed. Therefore, CRS could never find the DX's and would have to fall through until it found one of the DS's. With the DS's being decommissioned, this must be fixed.

CRS Build 12.0 splits the perl script into two. One continues to use TCP for the rdate time retrieval check. The new script uses ICMP to check for the echo port.

b. The AWIPS authorization file needs updating to include all DX's.

CRS Build 12.0 includes changes to postinstall script to include PX1, PX2, DX1, DX2, DX3, DX4, DS1, and DS2 in the AWIPS authorization file.

8. **TTR 976: Delete Voice Files From Messages Not Defined In Any Broadcast Suite** – A number of sites generate VIP voice files for remote sftp transmission, but do not broadcast those over any NWR transmitter. The recommended method for accomplishing this task is to send the message into CRS as an inactive message. However, some sites insist on sending the message to CRS by not including the message in any suite for transmitters on which the message is mapped to play. This accomplishes the same results as the inactive message method. However, prior to CRS Build 11.0, the voice files for messages not in any broadcast suite would stay on the hard drive forever unless manually deleted. Over time, this could fill up the FEPs and cause them to crash.

CRS Build 12.0 deletes the voice files of messages not scheduled in any broadcast suite.

BUG FIXES – VIP

1. **TTR 965: VIP MP3 Truncation Problems** – Prior to VIP Build 4.0, sometimes the VIP mp3 files were truncated. The problem was that the mp3 encoder executable and the DataTransfer script were running back-to-back. The DataTransfer script uses sftp to send the completed wave file back to CRS for scheduling. A temporary fix was made at North Platte where the problem was discovered. The temporary fix was to change the delay between the two scripts from 1 to 5 seconds. The delay increase allowed all of the mp3 data to be written

to disk before beginning the DataTransfer script.

VIP Build 4.0 changes the script to schedule the mp3 encoder and the DataTransfer script simultaneously.

2. **TTR 968: Remove VIP Unused IP Address Text Fields** – Prior to VIP Build 4.0, the VIP application contained a text field for the remote ftp server IP address, but this field was not used. Instead, the VIP application used the gateway entry in the /etc/hosts file.

VIP Build 4.0 removes the IP address text field boxes in the VIP Setup Wizard and the Audio FTP Configuration window.

3. **TTR 977: VIP CleanLogs Error in Cron** – The maintenance and runtime VIP log files are only removed when the disk image is restored. Over time, these log files too many are stored in the hard drive and they need to be cleaned up to keep the hard drive clean. The current VIP Version 3.2 software does include the VIPCleanLog script (TTR 896) which will run at 3:30am on the 2nd day of every month to clean these log files. However, the file entry for this script in the /etc/crontab file is incorrect preventing the removal of the old logs.

This was fixed in VIP Build 3.2.2, which is available for downloading from the NOAA4 server. It was manually fixed at all sites. VIP Build 4.0 fixes this problem permanently.