Service	Description	Type
LU09926	MQCHSUMM STATUS FIELD INCORRECT	PTF
LU09949	GSVC501P CICS STATE EXCEPTION MESSAGE INCORRECT	PTF
LU09999	IMS COMMANDS ENABLED FOR XSYSTEM/SYSTEM MODE	PTF
LU10014	JVMJNCK024E FATAL JVM JNI ERROR AND JVM$013E ZCN 0 APIS	*HIP/PRP*
LU10063	INVALID X'15' CHARACTER WHEN MLWTOENABLED IS SET TO NO	PTF
LU10067	GSVX390I GDBB BUFFFULL ISSUING IMSSPOC COMMAND	PTF
LU10096	GSV2325E PROFILE SYSTEM NOT DEFINED ISSUING LISTDIR	PTF
LU10154	SYSVUSER SERVER TASK LOOPS AFTER INVALID SRA PARAMETER	*HIP/PRP*
LU10229	SECURITY UPDATES NOT PICKED UP FOR SERVER SUBTASKS	PTF
LU10267	E-CSA OVERLAY RELATED TO MQ CHANNEL COLLECTION	**HIPER**
LU10287	SYSVAPPS MAINTENANCE	** PRP **
The CA RS 2306 service count for this release is 11		

FMID	Service	Description	Type
CNM4H00	LU09926	MQCHSUMM STATUS FIELD INCORRECT	PTF
	LU09949	GSVC501P CICS STATE EXCEPTION MESSAGE INCORRECT	PTF
	LU09999	IMS COMMANDS ENABLED FOR XSYSTEM/SYSTEM MODE	PTF
	LU10014	JVMJNCK024E FATAL JVM JNI ERROR AND JVM$013E ZCN 0 APIS	*HIP/PRP*
	LU10063	INVALID X'15' CHARACTER WHEN MLWTOENABLED IS SET TO NO	PTF
	LU10067	GSVX390I GDBB BUFFFULL ISSUING IMSSPOC COMMAND	PTF
	LU10096	GSV2325E PROFILE SYSTEM NOT DEFINED ISSUING LISTDIR	PTF
	LU10154	SYSVUSER SERVER TASK LOOPS AFTER INVALID SRA PARAMETER	*HIP/PRP*
	LU10229	SECURITY UPDATES NOT PICKED UP FOR SERVER SUBTASKS	PTF
	LU10267	E-CSA OVERLAY RELATED TO MQ CHANNEL COLLECTION	**HIPER**
	LU10287	SYSVAPPS MAINTENANCE	** PRP **

The CA RS 2306 service count for this FMID is 11

Service	Details
LU09926	LU09926 M.C.S. ENTRIES = ++PTF (LU09926) REWORK(2023132) MQCHSUMM STATUS FIELD INCORRECT PROBLEM DESCRIPTION: The Status field on the MQCHSUMM command display might be incorrect when running IBM MQ versions 9.1.0, 9.1.2 or 9.1.3. SYMPTOMS: The channel Status on the MQCHSUMM display shows INACTIVE when it is in a RUNNING state. You can verify the status by issuing the MQCHSTAT command to see the correct state. IMPACT: Incorrect status displays on the MQCHSUMM display. CIRCUMVENTION: Issue the MQCHSTAT command to display the correct status of the state. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20273 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00072-NM4170 DESC(MQCHSUMM STATUS FIELD INCORRECT). ++VER (Z038) FMID (CNM4H00) PRE (LU07313) SUP (LT09926)

Service	Details
LU09949	LU09949 M.C.S. ENTRIES = ++PTF (LU09949) REWORK(2023121) GSVC501P CICS STATE EXCEPTION MESSAGE INCORRECT PROBLEM DESCRIPTION: The CICS state exception WTO message GSVC501 contains the wrong action character suffix when the state metric has a Status of PROBLEM. All threshold and state exception messages (GSVC500/GSVC501 for CICS, and GSVX240/GSVX241 for other components) should use the following convention for the action character suffix, based on the metric new Status value: Char Metric Status ---- ---------- I NONE, NORMAL, UNKNOWN W HIGH, WARNING E PROBLEM SYMPTOMS: When a CICS state exception triggers, and the new metric Status is PROBLEM, the GSVC501 message has an action character suffix of 'P' instead of 'E': GSVC501P (SDCS) CICS_PIPELINE_Status Scope CICSPROD Name PIPE0001 Qual * State DISABLED NONE PROBLEM 0.000000 Policy 071BF380 Messages GSVC501I and GSVC501W are issued correctly as appropriate. IMPACT: Confusion regarding the action character, and might affect message automation processes. CIRCUMVENTION: None. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20288 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00074-NM4170 DESC(GSVC501P CICS STATE EXCEPTION MESSAGE INCORRECT). ++VER (Z038) FMID (CNM4H00) PRE (LU09347) SUP (LT09949) ++HOLD (LU09949) SYSTEM FMID(CNM4H00) REASON (AO) DATE (23121) COMMENT (+----------+ | SYSVIEW Performance Management Version 17.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | GSVC501P message ID change | +----------+----------+ |USERS | All users of SYSVIEW for CICS | |AFFECTED | | +----------+----------+

Service	Details
	|KNOWLEDGE	Product Administration
REQUIRED	| +----------+----------+ |ACCESS	Automation scripts
REQUIRED	| +----------+----------+ ********** * STEPS TO PERFORM * ********** If you have any automation around message GSVC501P, the message ID will be changing to GSVC501E. See following details: All threshold and state exception messages (GSVC500/GSVC501 for CICS, and GSVX240/GSVX241 for other components) should use the following convention for the action character suffix, based on the metric new Status value: Char Metric Status ---- ---------- I NONE, NORMAL, UNKNOWN W HIGH, WARNING E PROBLEM When a CICS state exception triggers, and the new metric Status is PROBLEM, the GSVC501 message has an action character suffix of 'P' instead of 'E', which is now being corrected: GSVC501P (SDCS) CICS_PIPELINE_Status Scope CICSPROD Name PIPE0001 Qual * State DISABLED NONE PROBLEM 0.000000 Policy 071BF380 Messages GSVC501I and GSVC501W are issued correctly as appropriate.).

Service	Details
LU09999	LU09999 M.C.S. ENTRIES = ++PTF (LU09999) REWORK(2023121) IMS COMMANDS ENABLED FOR XSYSTEM/SYSTEM MODE ENHANCEMENT DESCRIPTION: This feature PTF enhances the SYSVIEW Option for IMS by enabling additional commands for XSYSTEM and SYSTEM data mode. In addition, all XSYSTEM enabled IMS commands were standardized to use a common set of parameter keywords, similar to CICS and MQ command processing. This feature PTF contains the following enhancements and changes: 1. The following table documents the enhanced IMS commands and the common parameter keywords they support: Command SYSTEM XSYSTEM GROUP XSGROUP -------- ------ ------- ----- ------- IMSALERT Yes Yes Yes New IMSDAILY Yes Yes Yes New IMSDBASE New New New New IMSEVENT Yes Yes Yes New IMSLINES New New New New IMSLIST na Yes Yes New IMSLOCKS Yes Yes Yes New IMSLOGRS na Yes Yes New IMSLTERM New New New New IMSNODES New New New New IMSOVER na Yes Yes New IMSPROGS New New New New IMSPSBS New New New New IMSREGNS Yes Yes Yes New IMSSSYS New New New New IMSTIMES Yes Yes Yes New IMSTRANS New New New New IMSUEXIT New New New New IMSUSERS New New New New IMSWAITS Yes Yes Yes New New The functionality has been added with this feature. Yes The functionality already exists. na The functionality does not apply to the command (meaning the data is always returned in SYSTEM mode for the local system). 2. New profile variables IMSMODE and IMSGROUP were created to allow you to set a default MODE and GROUP for all IMS cross-system enabled commands. 3. A new XSPlex field was added to all of the IMS cross-system enabled commands showing the sysplex name from where the data was obtained. 4. A new JobT field was added to the IMSREGNS display to show the dependent region job type (STC, JOB, etc.) 5. All line commands from IMSREGNS are now supported for remote systems. Previously, some line commands might cause the following message to display: GSV2506E <lcmd> line command not supported for remote system <system> 5. IMSDAILY and IMSEVENT are now making security resource validation calls for the IMSID and IMSJOBN resources. The calls help to ensure that the user is authorized to see data for the selected IMS

Service	Details
	subsystem(s). PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20226 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00075-NM4170 DESC(IMS COMMANDS ENABLED FOR XSYSTEM/SYSTEM MODE). ++VER (Z038) FMID (CNM4H00) PRE (LU07568 LU07759 LU08271 LU08803 LU08900) SUP (LT07495 LT08972 LT09999 LU07495 LU08972) ++HOLD (LU09999) SYSTEM FMID(CNM4H00) REASON (ACTION) DATE (23121) COMMENT (+----------+----------+ | SYSVIEW Performance Management Version 17.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | To implement the fix. | +----------+----------+ |USERS | Users of the System Condition Monitor (SCM) | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Product administration | |REQUIRED | | +----------+----------+ |ACCESS | Product libraries | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** If you do not use the System Condition Monitor (SCM) then this HOLD can be ignored. To dynamically install this correction: 1. Apply this fix to update the IMOD source library CNM4BISR. 2. Use the sample IMODLOAD batch job, which can be found in the SAMPJCL and/or CNM4BSAM library, to load the new IMOD source into the ISET and compile it. Specify the following control statements in the IMODLOAD JCL: //SYSIN DD * PDSLOAD MEMBER GSVI0060 TO OUT FROM IN REPLACE IMOD SCM_IMSALERTS COMPILE IMOD SCM_IMSALERTS IN OUT STATUS PROD 3. Recycle GSSA to pick up these changes.).

Service	Details
LU10014	LU10014 M.C.S. ENTRIES = ++PTF (LU10014) REWORK(2023121) JVMJNCK024E FATAL JVM JNI ERROR AND JVM$013E ZCN 0 APIS PROBLEM DESCRIPTION: There are 2 problems resolved by this fix. 1. When the JVM option -Xcheck:jni:verbose is enabled in a JVM that is monitored by the SYSVIEW JVM agent, the JVM agent might cause the monitored JVM to shut down erroneously. When the option is enabled, using the JVMHEAPS, JVMMMGR, or JVMGC command in SYSVIEW to view information for the monitored JVM causes the shut down. Also, if the monitored JVM is a z/OS Connect server and the MonZcn option is passed to the SYSVIEW JVM agent, the JVM agent can fail during initialization and cause the z/OS Connect server to shut down. 2. When the SYSVIEW JVM agent is configured to monitor a z/OS Connect server that does not have any APIs defined and the MonZcnReq option is passed as enabled to the agent, the ZCNLIST and ZCNAPIS commands will display an error message. SYMPTOMS: 1. When the JVMHEAPS, JVMMMGR, or JVMGC command is used to display information for a monitored JVM with the -Xcheck:jni:verbose option enabled, or the monitored JVM is a z/OS Connect server with the -Xcheck:jni:verbose option enabled, the JVM shuts down and the following message appears in the JVM's job log: JVMJNCK024E JNI error detected. Aborting. 2. The following message appears on the ZCNLIST and ZCNAPIS displays: JVM$013E return code = 8 reason code = 12 IMPACT: 1. SYSVIEW JVM agent causes monitored JVM to shut down erroneously. 2. None. CIRCUMVENTION: 1. Disable the -Xcheck:jni:verbose option, or, add the nonfatal suboption The option string would look like -Xcheck:jni:verbose,nonfatal and causes JVM errors to be thrown but they will not cause the JVM to shut down. 2. Define at least one API in the z/OS Connect server. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 19923 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00077-NM4170 DESC(JVMJNCK024E FATAL JVM JNI ERROR AND JVM$013E ZCN 0 APIS). ++VER (Z038) FMID (CNM4H00) PRE (LU07602) SUP (FC07645 LT06849 LT10014 LU06849) ++HOLD (LU10014) SYSTEM FMID(CNM4H00) REASON (RESTART) DATE (23121) COMMENT (+----------+ | SYSVIEW Performance Management Version 17.0 | +----------+----------+ |SEQUENCE | After Apply |

Service	Details
	+----------+--+ |PURPOSE | To implement the fix | +----------+--+ |USERS | All users of SYSVIEW JVM monitoring | |AFFECTED | | +----------+--+ |KNOWLEDGE | Product Administration | |REQUIRED | | +----------+--+ |ACCESS | Product libraries | |REQUIRED | | +----------+--+ ********** * STEPS TO PERFORM * ********** If you do not use the JVM component then this HOLD can be ignored. 1. Apply the PTF. 2. Stop the JVMs configured to run the agent. Note that some address spaces such as CICS can have multiple JVMs. All JVMs in the address space must be stopped at the same time. 3. Stop the SYSVIEW STCs, GSSA, and any user sessions. 4. Deploy the agent run-time from the SMP/E managed directory "../cnm4h00/CNM4JVMD/" (DDDEF CNM4JVMD) to the run-time directory "../cnm4h00/runtime/". The deploy can be performed by running the install job sysviewhlq.SAMPJCL(INST0006). 5. Start the SYSVIEW STCs, GSSA, and any user sessions. 6. Start the JVMs configured to run the agent. Notes: 1. It is not required to immediately stop and start your JVMs to pick up the updated JVM data collector agent. A back-level agent will continue to communicate with a higher level SYSVIEW STC. It is recommended to keep the agent in sync with the SYSVIEW STC so the latest features and bug fixes are active in the agent. 2. The following SYSVIEW commands can be used to identify JVMs configured to run an agent that are currently running on a system: JVMARGS SYSTEM ; SELECT ARGUMENT CN -AGENTPATH Ensure all run-time directories are updated with the new binaries.). LINK('../libgsvoagt1.so') PARM(PATHMODE(0,7,7,5)). LINK('../libgsvoagt4.so') PARM(PATHMODE(0,7,7,5)).

Service	Details
LU10063	LU10063 M.C.S. ENTRIES = ++PTF (LU10063) REWORK(2023132) INVALID X'15' CHARACTER WHEN MLWTOENABLED IS SET TO NO PROBLEM DESCRIPTION: When the MlWtoEnabled option is set to NO in the OPTIONS parmlib member, messages written to SYSLOG might contain unprintable character x'15'. The x'15' represents a new line request. When a single line WTO is issued, the new line character should be translated to a space. However, it is not translated for all messages. SYMPTOMS: Possible no match when attempting to intercept SYSVIEW messages with automation. In the reported case MVS threshold messages contained the erroneous x'15' character, however CICS threshold messages did not. IMPACT: Unable to detect certain messages with automated operations. CIRCUMVENTION: Set the MlWtoEnabled option to YES to produce multi-line messages. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20383 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00078-NM4170 DESC(INVALID X'15' CHARACTER WHEN MLWTOENABLED IS SET TO NO). ++VER (Z038) FMID (CNM4H00) SUP (LT10063)

Service	Details
LU10067	LU10067 M.C.S. ENTRIES = ++PTF (LU10067) REWORK(2023124) GSVX390I GDBB BUFFFULL ISSUING IMSSPOC COMMAND PROBLEM DESCRIPTION: When issuing an IMS command, for example, IMSSPOC, the display data is not returned because the output buffer size that is required to accommodate the volume of data requested exceeds the maximum buffer size allowed. In the customer reported case, the IMSSPOC command was issued using a GROUP of type IMSSPOC, resulting in data being requested from multiple IMS subsystems. SYMPTOMS: There are no visible error messages returned. Only the following message appears in the user's LISTLOG: GSVX390I GDBB BuffFull. Total=01957800 Min=00032AF0 Max=01000000 Entries=25599 IMPACT: No data returned on the display. CIRCUMVENTION: Limit the display data to a smaller number of IMS subsystems. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20135 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00079-NM4170 DESC(GSVX390I GDBB BUFFFULL ISSUING IMSSPOC COMMAND). ++VER (Z038) FMID (CNM4H00) PRE (LU08900 LU09745) SUP (LT10067)

Service	Details
LU10096	LU10096 M.C.S. ENTRIES = ++PTF (LU10096) REWORK(2023128) GSV2325E PROFILE SYSTEM NOT DEFINED ISSUING LISTDIR PROBLEM DESCRIPTION: An error message is received when the LISTDIR command is issued with any of the directory type parameters, and the Dsn-System-PROFILE system configuration option is set to NONE. LISTDIR tries to determine if it was issued for the SYSVIEW profile data set, which allows the CHANGE, DPROFILE, and SWITCH line commands to work. In SYSVIEW 16.0, profile processing changed from using Dsn-System-PROFILE (PROFILE) to using Dsn-System-PROFLIB (PROFLIB). The new PROFLIB PDSE member names are not the actual names of the profiles as they were for PROFILE, so the CHANGE, DPROFILE, and SWITCH line commands will no longer work for PROFLIB. Therefore, these line commands will be deleted. SYMPTOMS: Issuing the LISTDIR command for any data set name other than what is specified on system configuration option Dsn-System-PROFILE causes the following error message to be issued: GSV2325E LibType PROFILE SYSTEM is not defined IMPACT: The error message is issued but the LISTDIR command still functions. CIRCUMVENTION: None. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20399 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00080-NM4170 DESC(GSV2325E PROFILE SYSTEM NOT DEFINED ISSUING LISTDIR). ++VER (Z038) FMID (CNM4H00) PRE (LU09745) SUP (LT10096) ++HOLD (LU10096) SYSTEM FMID(CNM4H00) REASON (DOC) DATE (23128) COMMENT (+----------+ | SYSVIEW Performance Management Version 17.0 | +----------+ ********** * PUBLICATION * ********** The following line commands are being removed from the LISTDIR command. They were only applicable when using LISTDIR against the old SYSVIEW PROFILE data set specified on the Dsn-System-PROFILE system configuration option. They will not work with the newer PROFLIB data set specified on the Dsn-System-PROFLIB system configuration option. CHANGE DPROFILE SWITCH).

Service	Details
LU10154	LU10154 M.C.S. ENTRIES = ++PTF (LU10154) REWORK(2023139) SYSVUSER SERVER TASK LOOPS AFTER INVALID SRA PARAMETER PROBLEM DESCRIPTION: When an invalid parameter keyword is passed to one of the following commands when called via the SYSVIEW REST API, the server subtask in the SYSVUSER address space that processed the request might enter a loop and become unresponsive. - CSIPROD (SYSVIEW 17.0) - KEYRINGS (SYSVIEW 17.0) - MODIDS (SYSVIEW 16.0 & 17.0) - PRODLIFE (SYSVIEW 17.0) - PTFS (SYSVIEW 16.0 & 17.0) See associated command help in SYSVIEW for each of the listed commands for a list of valid parameters that can be used. By default, the SYSVUSER address space starts five server tasks that can process REST API requests. If all of these tasks become unresponsive, the SYSVIEW REST API fails to respond to requests. The problem does not occur when these commands are entered via any interface other than the REST API. For example, ISPF, TSO, or VTAM. SYMPTOMS: Responses to SYSVIEW REST API requests are slow or timeout when issuing commands via the SYSVIEW REST API. The Listlog line command on the SRVRSTAT command shows the session log for the server tasks that process REST command requests. When viewing the log for the task that processed the invalid command request, the ActvCmd field on the LISTLOG command contains the primary command name that was passed an invalid parameter keyword and the following messages display: GSVX071E <keyword> is not a valid keyword for the <command> command GSVX054E*Invalid value for keyword After these messages, the REFRESH command is driven in a loop, indicated by the LISTLOG command displaying the values ENTERKEY in the Source field and REFRESH in the Data field. After each REFRESH, messages similar to the following appear in the server task's LISTLOG: GSVX903I SNDS$$ END GSVX903I GETR$$ END IMPACT: Slowdown in SYSVIEW REST API responses. Unable to use the SYSVIEW REST API if all server tasks in the SYSVUSER address space become unresponsive. High CPU usage may also be observed in the SYSVUSER address space. CIRCUMVENTION: To prevent the error, ensure that all impacted commands contain valid parameter keywords, when issued via the SYSVIEW REST API. If the error does occur, restart the SYSVUSER address space and the REST API becomes responsive. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20439 R00081-NM4170

Service	Details
	DESC(SYSVUSER SERVER TASK LOOPS AFTER INVALID SRA PARAMETER). ++VER (Z038) FMID (CNM4H00) PRE (LU08271 LU08900 LU09745) SUP (GC07645 LT10154)

Service	Details
LU10229	LU10229 M.C.S. ENTRIES = ++PTF (LU10229) REWORK(2023142) SECURITY UPDATES NOT PICKED UP FOR SERVER SUBTASKS PROBLEM DESCRIPTION: The SYSVUSER server subtasks that process REST API and Event Capture events had no mechanism to reset the security context used to process these requests. To address this, a MODIFY command was created for the SERVSEC task that forces a user id security context switch when the next request is processed, allowing any security changes to be picked up. To force a reset of the user id, issue the following command: MODIFY SYSVUSER,MODIFY SERVSEC,RESETUSERID <or> From the ASADMIN display, enter MODIFY in the line command field for the SERVSEC row, and fill the Parms field with RESETUSERID. The sample CNM4BPRM(SVWXSECC) parmlib member was updated to provide an example command to reset the user id automatically whenever an internal security update is detected. If external security is in use, issue the MODIFY command manually. SYMPTOMS: The user's access appeared to be unchanged after making an update to the internal or external security definitions. IMPACT: Unable to facilitate a security change. CIRCUMVENTION: From the ASADMIN display, STOP, then START the SERVSEC (Server Controller) task under SYSVUSER to force all servers to be restarted. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20452 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00082-NM4170 DESC(SECURITY UPDATES NOT PICKED UP FOR SERVER SUBTASKS). ++VER (Z038) FMID (CNM4H00) PRE (LU08271 LU08536 LU09745) SUP (LT10229) ++HOLD (LU10229) SYSTEM FMID(CNM4H00) REASON (DOC) DATE (23142) COMMENT (+--+ | SYSVIEW Performance Management Version 17.0 | +--+ ************************** * PUBLICATION * ************************** 'Communicate with the SYSVUSER Started Subtask' in the Administering section has been updated to document the MODIFY RESETUSERID command. 'CNM4BPRM - PARMLIB Members' in the Administering section has been updated for General Member SVWXSECC to provide a sample MODIFY

Service	Details
	RESETUSERID command.).

Service	Details
LU10267	LU10267 M.C.S. ENTRIES = ++PTF (LU10267) REWORK(2023144) E-CSA OVERLAY RELATED TO MQ CHANNEL COLLECTION PROBLEM DESCRIPTION: Possible overlay in CSA during SYSVIEW MQ Data collection can result in application or system outage. PROBLEM DESCRIPTION: An overlay in E-CSA might occur during SYSVIEW MQ channel collection, which can result in an application or system outage. Data might be written beyond the end of a common storage buffer used to gather MQ channel information. In SYSVIEW 16.0, this behavior can occur during data collection performed by the MQSDATA data collection subtask, or when issuing the MQCHAN or MQCHSTAT command. In SYSVIEW 17.0 this behavior can occur when issuing the MQCHAN or MQCHSTAT command. SYMPTOMS: Overlay of Common Storage area shows one or more blocks beginning with an eyecatcher of 'QSRSE' and containing MQ channel names. IMPACT: Unpredictable results. Possible application or system outage due to the overlay. CIRCUMVENTION: In SYSVIEW 17.0, temporarily disable the MQCHAN and MQCHSTAT commands using security or the CMDATTR parmlib member. In SYSVIEW 16.0, in addition to disabling those two commands, also disable the MQSDATA-CHANNELS data collection function using the DIS line command on the SCHEDULE command. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20415 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00083-NM4170 DESC(E-CSA OVERLAY RELATED TO MQ CHANNEL COLLECTION). ++VER (Z038) FMID (CNM4H00) SUP (LT08071 LT10267 LU08071)

Service	Details
LU10287	LU10287 M.C.S. ENTRIES = ++PTF (LU10287) REWORK(2023150) SYSVAPPS MAINTENANCE PROBLEM DESCRIPTION: This PTF updates the SYSVIEW REST Server (SYSVAPPS) to the latest maintenance. The following updates are included in this PTF: 1. When using z/OSMF JWTs to authenticate, it is possible that the truststore defined in the application.yml config file is not used. Instead, the truststore located at $JAVA_HOME/security/cacerts may be used. This can prevent users from being able to make requests. 2. Update all third-party software dependencies to the latest versions. The update includes all packages which have had vulnerabilities reported. Note that the SYSVIEW REST server does NOT meet the requirements for any currently reported CVE, and is therefore NOT vulnerable. Specifically, the following vulnerabilities are mitigated: Spring Boot: 2023-20873 Spring Security: 2022-20862 Spring Framework: 2022-20863,2022-20861,2022-20860 Jettison - Json Stax implementation: 2023-1436 This is a proactive step for ease of mind, as threats might still be reported when running a scan on the SYSVAPPS JAR file. SYMPTOMS: 1. Incorrect truststore is used, leading to authentication issues. 2. When running vulnerability scans against the SYSVAPPS JAR file, false alarms might trigger. IMPACT: 1. Unable to use z/OSMF JWTs to authenticate. 2. Unnecessary concern about whether the SYSVAPPS REST server is secure. CIRCUMVENTION: None. PRODUCT(S) AFFECTED: SYSVIEW Performance Management Version 16.0 SYSVIEW Performance Management Version 17.0 Related Problem: SYSVW 20545 (C) 2023 Broadcom Inc and/or its subsidiaries; All rights reserved R00084-NM4170 DESC(SYSVAPPS MAINTENANCE). ++VER (Z038) FMID (CNM4H00) PRE (LU07917 LU08271 LU09628) SUP (AL07917 LT10287) ++HOLD (LU10287) SYSTEM FMID(CNM4H00) REASON (RESTART) DATE (23150) COMMENT (+----------+ | SYSVIEW Performance Management Version 17.0 | +----------+----------+ |SEQUENCE | After Apply | +----------+----------+ |PURPOSE | To implement the fix | +----------+----------+ |USERS | All users of the SYSVIEW REST API |

Service	Details
	|AFFECTED | |
	+----------+--+
	|KNOWLEDGE | Product Administration |
	|REQUIRED | |
	+----------+--+
	|ACCESS | Product libraries |
	|REQUIRED | |
	+----------+--+
	**************************
	* STEPS TO PERFORM *
	**************************
	After applying this PTF, the Application Server run-time directories
	will need to be deployed to your site's run-time environment. Follow
	these steps to implement the change:
	1. Stop the SYSVAPPS task (P SYSVAPPS).
	2. Copy the SMP/E managed directories to the run-time directories
	by running the smpehlq.SAMPJCL(MAINT009) sample JCL. You will
	need to set PATHPFX to the USS directory path prefix used for
	installation (see comments in the JCL).
	3. Start the SYSVAPPS task (S SYSVAPPS).
	).
	LINK('../libbcm-apisdk-attls.so') PARM(PATHMODE(0,7,7,5)).
	LINK('../SYSVIEW-app-server.jar') PARM(PATHMODE(0,7,7,5)).
	LINK('../libbcm-apisdk-security.so') PARM(PATHMODE(0,7,7,5)).
	MCS LU09926 STARTS ON PAGE 0002
	MCS LU09949 STARTS ON PAGE 0002
	MCS LU09999 STARTS ON PAGE 0004
	MCS LU10014 STARTS ON PAGE 0008
	MCS LU10063 STARTS ON PAGE 0011
	MCS LU10067 STARTS ON PAGE 0012
	MCS LU10096 STARTS ON PAGE 0013
	MCS LU10154 STARTS ON PAGE 0014
	MCS LU10229 STARTS ON PAGE 0016
	MCS LU10267 STARTS ON PAGE 0017
	MCS LU10287 STARTS ON PAGE 0018

Product Family	Product	Release
Performance and Storage	SYSVIEW PERFORMANCE MANAGEMENT	17.00.00

The CA RS 2306 Product/Component Count for this release is 1

CA RS Level	Service	FMID
CAR2306	LU10287	CNM4H00
	LU10267	CNM4H00
	LU10229	CNM4H00
	LU10154	CNM4H00
	LU10096	CNM4H00
	LU10067	CNM4H00
	LU10063	CNM4H00
	LU10014	CNM4H00
	LU09999	CNM4H00
	LU09949	CNM4H00
	LU09926	CNM4H00
CAR2305	LU09995	CNM4H00
	LU09928	CNM4H00
	LU09775	CNM4H00
	LU09757	CNM4H00
	LU09745	CNM4H00
	LU09732	CNM4H00
	LU09628	CNM4H00
	LU09521	CNM4H00
	LU09414	CNM4H00
CAR2304	LU09711	CNM4H00
	LU09668	CNM4H00
	LU09636	CNM4H00
	LU09561	CNM4H00
	LU09500	CNM4H00
	LU09367	CNM4H00
	LU09347	CNM4H00
	LU09265	CNM4H00
	LU09029	CNM4H00
CAR2303	LU09156	CNM4H00
	LU09124	CNM4H00
	LU09061	CNM4H00
	LU09050	CNM4H00
	LU08994	CNM4H00
	LU08972	CNM4H00
	LU08900	CNM4H00
	LU08681	CNM4H00
	LU08333	CNM4H00
CAR2302	LU08961	CNM4H00
	LU08874	CNM4H00
	LU08803	CNM4H00
	LU08663	CNM4H00
CAR2301	LU08542	CNM4H00
	LU08536	CNM4H00
	LU08378	CNM4H00
	LU08362	CNM4H00
	LU08111	CNM4H00

CA RS Level	Service	FMID
	LU07707	CNM4H00
CAR2212	LU08294	CNM4H00
	LU08292	CNM4H00
	LU08271	CNM4H00
	LU08071	CNM4H00
	LU08011	CNM4H00
	LU07933	CNM4H00
	LU07917	CNM4H00
	LU07888	CNM4H00
	LU07796	CNM4H00
	LU06852	CNM4H00
CAR2211	LU07870	CNM4H00
	LU07759	CNM4H00
	LU07727	CNM4H00
	LU07693	CNM4H00
	LU07671	CNM4H00
	LU07661	CNM4H00
	LU07607	CNM4H00
	LU07602	CNM4H00
	LU07579	CNM4H00
	LU07573	CNM4H00
	LU07568	CNM4H00
	LU07528	CNM4H00
	LU07310	CNM4H00
	LU07136	CNM4H00
	LU06849	CNM4H00
CAR2210	LU07495	CNM4H00
	LU07410	CNM4H00
	LU07378	CNM4H00
	LU07371	CNM4H00
	LU07350	CNM4H00
	LU07313	CNM4H00
CAR2209	LU07044	CNM4H00
	LU07009	CNM4H00
	LU06861	CNM4H00
	LU06816	CNM4H00