IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium patch 11.0p470
Name of file:	SqlGuard-11.0p470_Bundle_Mar_22_2023.tgz.enc.sig
MD5SUM:	a5747104fc76657bf85f4d03894add65
Release:	20 March 2023

Finding the Patch

This document is intended to provide a reference to the contents of this patch. If applicable, the detailed description of each fix and instructions for applying this patch are contained within the download package available at the IBM Fix Central website at http://www.ibm.com/support/fixcentral/.

Make the following selections on Fix Central:

- Product selector: IBM Security Guardium
- Installed Version: 11.0
- Platform: UNIX/Linux/Windows
- Click “Continue”, then select “Browse for fixes” and click “Continue” again.
- Select “Appliance Patch (GPU and ad hoc)”

Prerequisites:

- Guardium 11.0p400. See patch release notes for 400
- The latest health check patch 11.0p9997

Notes:

- Patch 11.0p470 is an appliance bundle that includes all fixes for 11.4 except sniffer fixes.
- This patch restarts Guardium system.
- Download the patch and extract the compressed package outside the Guardium system.
- Pick a quiet time on the appliance.
- Apply the latest health check patch.
- Install the patch in a top-down manner on all appliances, starting with the central manager, then aggregators, and then the collectors.

For information on Guardium patch types and naming convention, see:
https://www.ibm.com/support/pages/node/6195371

Enhancements

Issue Key	Description
GRD-64866	Enhance VA Available test report – add attack vector- attack vector and cvss score are added to "Available VA tests – detailed" report
GRD-62518	Improvements in drops in priority queue- Guardium now avoids drops for priority packets
GRD-62010	Added Analyzer Queue Drops and Priority Queue Drops columns to Buff Usage Monitor report and Enterprise Buff Usage Monitor report
GRD-46868	Automated the *add_domain_to_universal_connector_allowed_domains* grdapi that was previously required during S3 configuration. This simplifies the workflow.
GRD-65541	The Guardium alerter now sends an SNMP trap with a new specification. Accordingly, there is a new Guardium MIB file for deployment to SNMP servers to allow the changed traps to be understood. To allow an SNMP server to understand the Guardium SNMP trap, deploy the GUARDIUM-TRAP-V2-MIB.txt file along with this bundle. Then, load the .txt file into the SNMP server separately. The file is available on Fix Central as " Guardium_SNMP-Trap-V2-MIB". It is not a part of this bundle and does not need to be deployed to the appliance.
GRD-56535	You can now install the AWS CloudWatch agent on AWS Guardium AMIs instead of using Syslog

Bug Fixes

Patch	Issue key	Summary	APAR
11.0p440		Link to patch 11.0p440 in Fix Central	
11.0p450		Link to patch 11.0p450 in Fix Central	
11.0p460		Link to patch 11.0p460 in Fix Central	
11.0p470	INS-26532	GI Datamart Activation Not Working	GA18223
	GRD-69230	Classification count (*) causing timeouts	GA18257

		For Oracle data sources, Guardium now supports using database statistics to determine cardinality when the classifier uses random sampling. For more information, see the DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS custom property in the following documentation: https://ibm.com/docs/en/SSMPHH_11.4.0?topic=datasource-oracle-data-direct-service-name https://ibm.com/docs/en/SSMPHH_11.4.0?topic=datasource-oracle-data-direct-sid	
	GRD-68013	Generate GUI CSR without the OU field	GA18213
	GRD-67346	Show service state for 8444 erroneously shows enabled, even if disabled	GA18220
	GRD-67338	MS Azure SQL Database Cloud Connection Issue	GA18229
	GRD-67250	store sync_solr_certificate sets expiration date to 01/23/2023 causing alert on GUI	GA18156
	GRD-67119	Data Source User Name field is limited to 50 characters	GA18155
	GRD-67028	Getting error "Invalid argument resultSetType, use TYPE_FORWARD_ONLY " when trying to get a roles assigned report in a SAP HANA DB	GA18215
	GRD-66966	Unable to reset an accessmgr account that is disabled.	GA18185
	GRD-66956	Password expiration for GUI is reset to default 90 days after applying patch	GA18181
	GRD-66878	ServiceNow is not loading Assignment group, Category Subcategory Affected CI and Environment fields for a new ticket created in Guardium Threat Analytics integration	GA18224
	GRD-66858	System Data Backup error: mysqldump: Error 1412: Table definition has changed, please retry transaction when dumping table `TURBINE_USER_GROUP_ROLE`	GA18151
	GRD-66752	Old data in GDM_SESSION table is not purged and partitions are not deleted	N/A
	GRD-66672	MSSQL DB having issues with SGATE and Session Level Policy	N/A
	GRD-66544	Inconsistent External S-TAP Load Balancing options listed on the GUI	GA18187

	GRD-66429	networkaddress.cache.ttl value in java.security got overwritten by patch bundle (e.g. P450)	GA18221
	GRD-66283	Aggregation/Archive report indicates success when purge fails	N/A
	GRD-65923	Classification timeout repeating more times on same object	GA18165
	GRD-65772	Active Threat Analytics - Source Behavioral Analysis is EMPTY in all incidents	GA18189
	GRD-65746	Issues identified post Event Hub implementation in Azure environment	GA18166
	GRD-65689	STAP 'Missing parameters' in 'Run diagnostics' of 'Module Installation/Set up by Client'	GA18194
	GRD-65640	Distributed Report does not complete for one date with a lot of traffic	GA18173
	GRD-65541	Need MIB file for SNMP Traps	GA18206
	GRD-65342	grdapi create_datasource does not store secret name	GA18143
	GRD-65312	Custom Table Scheduling section missing with Datasource using Cyberark	GA17811
	GRD-65280	Include all rolled-over ELB logs in ELB must gather	N/A
	GRD-65189	Multiple Scheduled Audit Processes Not being executed	GA18188
	GRD-65119	Errors in discovery data	GA18231
	GRD-65081	Query-Report Builder takes a lot of time to save queries	GA18209
	GRD-65026	After cli password expires when changing to new password guardium cli forces to change the password twice instead of once	GA18118
	GRD-64972	Error "cannot register unit at this time. Invalid shared secret" registering managed unit from the GUI	GA17645
	GRD-64885	Cannot create a report with TotalAccess field in condition	N/A
	GRD-64149	ERR=880 TRYING TO UPDATE A VULNERABILITY ASSESSMENT TEST EXCEPTION GROUP USING GRDAPI	GA18167
	GRD-64077	SNMP commands output error after patch upgrade	GA18172
	GRD-63504	Add groups has Errors in the Database	GA18084
	GRD-63406	Inactive Universal Connector Oracle Unified Auditing (OAU) connections showing up in Stap Status Monitor Page	GA18120

	GRD-62057	S-TAP verification failed even the datasource test connection is successful	GA18102
	GRD-56003	Quick Search shows enabled in GUI and CLI but Investigation DB says it's not enabled	GA17763
	GRD-55293	Failing Backup jobs in Guardium - ERROR: Backup file was not copied. Method=TSM	GA17822
	GRD-52978	SOFTWARE_TAP_PROPERTY_HISTORY table crashing multiple times on multiple appliance(Need RCA)	GA18216

Known Limitations

Issue Key	Description
GRD-54393	UC status is disabled on an upgraded env (11.4 -> 11.5). **Workaround:** Enable UC from GUI.
GRD-57381	Historical data files for v3 datamarts exception, sentence, session log, session log end were not exported to GI cluster, error 'No connection info'. This issue is present in v11.3 and v11.4 and will be fixed in v11.5.
GRD-64679	Installing this bundle changes the schedule time for threat finder. The schedule time does not update automatically after bundle installation. **Workaround:** Update the schedule manually by disabling and re-enabling threat finder after installing this bundle.

Security Fixes

Issue key	Summary	CVEs
GRD-69219	PSIRT: PVR0427712, PVR0427713 - krb5 - CVE-2022-42898, CVE-2021-37750 (Publicly disclosed vulnerability)	**CVE-2022-42898**
GRD-66526	PSIRT: PVR0406994 - postgresql-42.2.20.jar (Publicly disclosed vulnerability found by Mend)	CVE-2022-41946
GRD-66356	PSIRT: PVR0404423, PVR0404947 - IBM SDK, Java Technology Edition Quarterly CPU - Oct 2022 - Includes Oracle October 2022 CPU and IBM Java - OpenJ9	CVE-2022-21628 CVE-2022-21626 CVE-2022-21624 CVE-2022-21619 CVE-2022-3676
GRD-66000	PSIRT: PVR0405173 - Pen Testing 2022 - Using Components with Known Vulnerabilities - OS Components	CVE-2020-0465 CVE-2020-0466 CVE-2021-0920 CVE-2021-3564

		CVE-2021-3573 CVE-2021-3752 CVE-2021-4155 CVE-2022-0330 CVE-2022-22942 CVE-2022-40674 CVE-2022-41974 CVE-2019-18282 CVE-2020-10769 CVE-2020-14314 CVE-2020-14385 CVE-2020-24394 CVE-2020-25212 CVE-2020-25643 CVE-2020-26137 CVE-2022-29154 CVE-2022-2526 CVE-2022-31676
GRD-65856	PSIRT: PVR0398504 - reactor-netty-http-1.0.13.jar (Publicly disclosed vulnerability found by Mend)	CVE-2022-31684
GRD-65349	PSIRT: PVR0393990 - hsqldb-2.3.2.jar (Publicly disclosed vulnerability found by Mend) - jetspeed	CVE-2022-41853
GRD-65348	PSIRT: PVR0393990 - hsqldb-2.3.2.jar (Publicly disclosed vulnerability found by Mend) - fam-crawler	CVE-2022-41853
GRD-63351	PSIRT: PVR0374433 - aws-java-sdk-s3-1.11.344.jar (Publicly disclosed vulnerability found by WhiteSource) - webapps	CVE-2022-31159
GRD-62530	PSIRT: PVR0292319 - [All] kernel - CVE-2021-3715 (Publicly disclosed vulnerability) - kpatch	CVE-2021-3715
GRD-59831	PSIRT: PVR0316527, PVR0325276, PVR0344948, PVR0374447 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - jackson-databind-2.10.0.jar - TSM - Dep Delay Exception	CVE-2020-25649 CVE-2020-36518
GRD-58022	PSIRT: PVR0316540 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - httpclient-4.5.10.jar - Dep Delay Exception	CVE-2020-13956
GRD-58000	PSIRT: PVR0309377 - PEN-TEST: Privilege Escalation in IBM Security Guardium - multiple locations	CVE-2021-39071
GRD-65520	PSIRT: PVR0395408, PVR0404220, PVR0404208 - protobuf-java-2.4.1.jar (Publicly disclosed vulnerability found by Mend) - SOLR	CVE-2022-3171 CVE-2022-3510 CVE-2022-3509
GRD-65519	PSIRT: PVR0395408, PVR0404220, PVR0404208 - protobuf-java-2.4.1.jar (Publicly disclosed vulnerability found by Mend) - webapps	CVE-2022-3171 CVE-2022-3510 CVE-2022-3509

GRD-65518	PSIRT: PVR0395408, PVR0404220, PVR0404208 - protobuf-java-2.4.1.jar (Publicly disclosed vulnerability found by Mend) - datastreams	CVE-2022-3171 CVE-2022-3510 CVE-2022-3509