IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium patch 11.0p525
Name of file:	SqlGuard-11.0p525_Bundle_May_18_2023.tgz.enc.sig
MD5SUM:	a9d0c18c9de406bc32984f7924456f01
Release:	24 May 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: 11.500
- Platform: UNIX/Linux/Windows
- Click “Continue”, then select “Browse for fixes” and click “Continue” again.
- Select “Appliance Patch (GPU and ad hoc)”

Prerequisites:

- Guardium 11.0p500
- The latest health check patch 11.0p9997

Notes:

- Patch 11.0p525 is an appliance bundle that includes all fixes for 11.5 except sniffer fixes.
- This patch restarts the 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.
- **Note: in patch 11.0p525, the store wkc_certificate command is renamed to store certificate wkc.**
- **Note: after installing this patch, install Guardium ad-hoc patch 11.0p1235. See here for more details.**

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

Enhancements

Issue Key	Description
GRD-47676	The Report Builder now has expanded functionalities, such as more automated checks and tracking for compressions levels and Exclude IP.

Bug Fixes

Patch	Issue key	Summary	APAR
11.0p5		Link to 11.5 in Fix Central	
11.0p510		Link to 11.510 in Fix Central	
11.0p520		Link to 11.520 in Fix Central	
11.0p525	INS-26532	GI Datamart Activation Not Working	GA18223
	GRD-71129	CLI Command difference for store wkc_certificate in 525	
	GRD-70155	guardium appliance unexpected behavior after daylight saving time changes in Egypt	GA18267
	GRD-69920	After upgrade 11.5 In Report Section Datasource Report taking longer time to display Database inventory	GA18281
	GRD-68013	Generate GUI CSR without the OU field	GA18213
	GRD-67720	Scheduled Job Exception every hour PEStatusJob trigger	GA18214
	GRD-67699	"show network verify" command on Microsoft Azure hosted Guardium appliance does not work.	GA18237
	GRD-67338	Connection to Microsoft Azure SQL Datasource on Cloud fails	GA18229
	GRD-67265	SAML Authentication error dialog appears when login via W3, then users are directed to CM Welcome page.	
	GRD-67119	Data Source User Name field is limited to 50 characters	GA18155

	GRD-67093	Report Color Indication Rule with 'In Group'/'Not In Group' Not Working Properly	GA18240
	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-66984	After GPU 500 installation the GUI is not started when uses non-default port (8443)	GA18232
	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-66920	After upgrade 11.5 In Report Section Datasource Report taking longer time to display Database inventory	GA18281
	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-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-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-65119	Errors in discovery data	GA18231
	GRD-65081	Query-Report Builder takes a lot of time to save queries	GA18209
	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-64883	Guardium Memory utilization SNMP MIBs	GA18241

	GRD-62057	S-TAP verification failed even the datasource test connection is successful	GA18102
	GRD-59740	Custom query based on a distributed report gets scrambled if the columns order of the distributed report is changed	GA17617
	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-70827	In Chrome/Edge, when opening the Investigation Dashboard from Risk Spotter and Active Threat Analytics pages, the Investigation dashboard opens with a default search and not with the correct filters. **Workaround:** Use Firefox to open the Investigation dashboard. Alternatively, (a) leave the Investigation dashboard window open, (b) repeat the UI action that you want, and (c) switch to the already opened Investigation dashboard search window.
GRD-71262	When saving an edit query with the TotalAccess field in condition, the query is saved but the UI does not indicate this. **Workaround:** The query is saved, even though the UI does not indicate this. This will be fixed in upcoming releases.

Security Fixes

Issue key	Summary	Custom field (CVEs)
GRD-68168	PSIRT: PVR0417768 - IBM Security Guardium - Oracle MySQL vulnerabilities	CVE-2023-21881 CVE-2023-21875 CVE-2023-21877 CVE-2023-21871 CVE-2023-21867 CVE-2023-21863 CVE-2023-21860 CVE-2023-21880 CVE-2023-21874

		CVE-2023-21870 CVE-2023-21866 CVE-2023-21865 CVE-2023-21883 CVE-2023-21840 CVE-2023-21879 CVE-2023-21873 CVE-2023-21869 CVE-2023-21868 CVE-2023-21864 CVE-2023-21882 CVE-2023-21876 CVE-2023-21836 CVE-2023-21878 CVE-2023-21872
GRD-68167	PSIRT: PVR0417772 - IBM Security Guardium is vulnerable to sudo - CVE-2023-22809 (Publicly disclosed vulnerability)	CVE-2023-22809
GRD-67229	PSIRT: PVR0412784 - IBM Security Guardium is vulnerable to a Insufficient Session Expiration vulnerability	243657
GRD-67023	PSIRT: PVR0412782 - Guardium V11.5 affected by "Reverse Tabnabbing" Vulnerability	GA18239
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-66002	PSIRT: PVR0405174 - Pen Testing 2022 - Using Components with Known Vulnerabilities - wire-grpc-server-generator	CVE-2021-41100 CVE-2018-8909 CVE-2021-41119
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-60285	PSIRT: PVR0344948, PVR0254469 - jackson-databind-2.12.6.jar (Publicly disclosed vulnerability found by WhiteSource) - zookeeper Dep Delay Exception - Solr	CVE-2020-36518 CVE-2021-20190
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