IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium patch 11.0p380
Name of file:	SqlGuard-11.0p380_Bundle_Feb_17_2023.tgz.enc.sig
MD5SUM:	df95f0c5a6bb3cd2731c99b25f93deb6
Release:	6 February 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 11.0p300. See patch release notes for 300
- The latest health check patch 11.0p9997

Notes:

- Patch 11.0p380 is an appliance bundle that includes all fixes for 11.3 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

New Features

Issue key	Summary
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

Known Limitations

Issue Key	Description
GRD-65622	Intermittent_Unable to add permissions to the role for "Reports", only on Microsoft Edge browser
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.
GRD-64271	Create New Discovery Scenario page is taking more than a minute to load. The fix will be included in upcoming releases
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'
GRD-65038	When accessing GIM and STAP dashboard, intermittently an error might be generated. The fix will be included in upcoming releases

Bug Fixes

Patch	Issue key	Summary	APAR
11.0p370		Link to patch 11.0p370 in Fix Central	
11.0p372		Link to patch 11.0p372 in Fix Central	
11.0p375		Link to patch 11.0p375 in Fix Central	
11.0p380	GRD-66544	Inconsistent External S-TAP Load Balancing options listed on the GUI	GA18187

	GRD-66283	Aggregation/Archive report indicates success when purge fails	N/A
	GRD-65772	Active Threat Analytics - Source Behavioral Analysis is EMPTY in all incidents	GA18189
	GRD-65689	STAP 'Missing parameters' in 'Run diagnostics' of 'Module Installation/Set up by Client'	GA18194
	GRD-65668	Fileserver doesn't work after setting "store cipher java secure"	GA18149
	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-64573	Error during classification scan: Cursors are not supported on a table which has a clustered columnstore index	GA18140
	GRD-64077	SNMP commands output error after patch upgrade	GA18172
	GRD-63504	Add groups has Errors in the Database	GA18084
	GRD-62983	Backup CONFIG Failed on p440 Upgraded Appliances	GA18075
	GRD-62057	S-TAP verification failed even the datasource test connection is successful	GA18102
	GRD-68884	Getting Warnings while enabling ecosystem	N/A

Security Fixes

Issue key	**Summary**	**CVEs**
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-65856	PSIRT: PVR0398504 - reactor-netty-http-1.0.13.jar (Publicly disclosed vulnerability found by Mend)	CVE-2022-31684
GRD-65696	PSIRT: PVR0398907 - x11 org out of bounds vulnerability	CVE-2022-2319 CVE-2022-2320
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-65050	PSIRT: PVR0389954 - kafka-clients-2.8.1.jar (Publicly disclosed vulnerability found by Mend) - GuardReqs	CVE-2022-34917
GRD-65049	PSIRT: PVR0389954 - kafka-clients-2.8.1.jar (Publicly disclosed vulnerability found by Mend) - Platform	CVE-2022-34917
GRD-65048	PSIRT: PVR0389954 - kafka-clients-2.8.1.jar (Publicly disclosed vulnerability found by Mend) - GlobalUtils	CVE-2022-34917
GRD-65047	PSIRT: PVR0389954 - kafka-clients-2.8.1.jar (Publicly disclosed vulnerability found by Mend) - datastreams	CVE-2022-34917
GRD-64376	PSIRT: PVR0386293 - IBM Security Guardium has an information exposure vulnerability	CVE-2022-39166
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-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