IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium patch 11.0p375
Name of file:	SqlGuard-11.0p375_Bundle_Oct_19_2022.tgz.enc.sig
MD5SUM:	d2d58bda640b9e48935c32ac9cd3446
Release:	28 October 2022

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 11.0p375 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.
- **Update to criteria for days to be purged**
  In the case where 'Allow purge without exporting or archiving' is not selected. After installing this patch, days which meet these criteria will now be purged:
  - **The day is older than the purge age + 60 days**
  - **The day has not been exported or archived**
  - **The day contains data only in one or more of Message, Message Text and Exception entities**

- **This change allows automatic purging of old days that do not contain audit data, preventing data building up on the appliance. If the data is only in Message, Message Text and Exception entities it means that data is from internal Guardium alerts. In many cases they have been generated on the appliance before export or archive was scheduled.**
- **If your appliance contains days that meet the new criteria, the first purge after installing this patch will delete those days and might take longer than expected. After the first purge the old data will be cleaned up and the process should run as normal.**
- **To investigate if you have any old days not exported or archived before installing this patch, use report 'Days not exported or archived' from Query-report builder - https://www.ibm.com/docs/en/guardium/11.4?topic=mdarasb-viewing-days-whose-data-was-not-archived-exported**

- **Note: CyberArk customers who have currently installed CyberArk must do the following to establish a connection with CyberArk:**
  1. Run the CLI command "show cyberark status" to see if CyberArk has been installed.
  2. If CyberArk has been installed, run the CLI command "store cyberark uninstall" to uninstall Cyberark.
  3. Then, install the new CyberArk patch 1014. Afterwards, run the CLI command "store cyberark install" to install CyberArk.
  4. See the "CyberArk version download" table below for expanded guidance on which patch you need to install.

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

Enhancements

Patch 11.0p375 includes several enhancements to the Venafi certificate management feature. You can now use grdAPI commands to propagate Venafi configurations and certificates from a central manager to some or all of the managed units. For more information, see Managing certificates by using Venafi.

New Features

Issue key	Summary
GRD-63619	**New health check feature** New status for health check v11.0p9997 has been added. In cases where there is an issue for v11.5 and above GPU installation, patch install status for p9997 can show "WARNING: Review health check log file.". If upgrading to v11.5 or above and this status is seen, health check log should be reviewed. See the v11.0p9997 release notes for more details.
GRD-60386	**CyberArk** Guardium now supports the CyberArk AIM agent version 12.4.1.

	To obtain the installation file SqlGuard-11.0p1014.tgz.enc.sig (CyberArk patch 11.0p1014), you must contact IBM support by opening an IBM support case at the following link: https://www.ibm.com/mysupport/s/?language=en_US. Install the new AIM agent by using the following procedure: 1) Download the SqlGuard-11.0p375_Bundle_Oct_19_2022.tgz.enc.sig (patch 11.0p375) from the IBM Fix Central website and install it on your Guardium system. 2) If the CyberArk AIM agent is running, uninstall it by using the CLI command `store cyberark uninstall` 3) Install the file **SqlGuard-11.0p1014.tgz.enc.sig** (CyberArk patch 11.0p1014) on your Guardium system 4) Install the CyberArk AIM agent by using the CLI command `store cyberark install` Note: After you install the new CyberArk patch, the Guardium system indicates that CyberArk version 12.04 is installed. Version 12.04 is the Guardium equivalent of CyberArk AIM agent 12.4.1. If you had previously configured your datasources to connect to CyberArk, you need not reconfigure them. Test a datasource to ensure that your Guardium system can establish a connection and fetch the password from your CyberArk vault. For more information on how to install CyberArk, see Deploying Cyberark on your Guardium system.

Known Limitations

Issue Key	Description
GRD-65622	Intermittent_Unable to add permissions to the role for "Reports", only on Microsoft Edge browser
GRD-64792	A warning appears in the CLI to show a certificate summary. This can be disregarded.
GRD-64679	ATA cases not generated when the process runs before the period for threat finder. The fix will be included in upcoming releases.
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.
GRD-66158	Unable to add Inspection Engine from GUI (STAP Control page) for Windows STAPs.

	Workaround: use grdapi command to add Inspection Engine for Windows STAP. Fix for GUI will be provided in upcoming releases.

Bug Fixes

Patch	Issue key	Summary	APAR
11.0p360		Link to patch 11.0p360 in Fix Central	
11.0p370		Link to patch 11.0p370 in Fix Central	
11.0p372		Link to patch 11.0p372 in Fix Central	
11.0P375	GRD-64052	Unable to Open Ticket to Resilient	GA18123
	GRD-63586	Snif restarting while sending OUA credentials to S-TAP	GA18115
	GRD-63441	v11.4 Additional SSIS Vulnerabilities Appearing after installing SSIS	GA18108
	GRD-62618	Blank "Last Connect" field in "Data-Sources" report for CouchDB datasources	GA18016
	GRD-62057	S-TAP verification failed even the datasource test connection is successful	GA18102
	GRD-60445	Audit process not writing results to SYSLOG p410	GA18017
	GRD-56003	Quick Search shows enabled in GUI and CLI but Investigation DB says it's not enabled	GA17763
	GRD-50650	Cannot grant privileges to a Role on all Guardium reports due error: "Unable to connect to UI server. Verify that server is operational and try again."	GA17588

Security Fixes

Issue key	Summary	CVEs
GRD-63353	PSIRT: PVR0375541, PVR0375714 - [All] Oracle MySQL (Publicly disclosed vulnerability) - July 2022 CPU	CVE-2022-21522 CVE-2022-21530 CVE-2022-21509 CVE-2022-21455 CVE-2022-21526 CVE-2022-21527 CVE-2022-21531 CVE-2022-21517 CVE-2022-21519

		CVE-2022-21528 CVE-2022-21515 CVE-2022-21525 CVE-2022-21529 CVE-2022-21538 CVE-2022-21556 CVE-2022-21547, CVE-2022-21534 CVE-2022-21537 CVE-2022-21553, CVE-2022-21555 CVE-2022-21535 CVE-2022-21550 CVE-2022-21569 CVE-2022-21539
GRD-62530	PSIRT: PVR0292319 - [All] kernel - CVE-2021-3715 (Publicly disclosed vulnerability) - kpatch	CVE-2021-3715
GRD-62345	PSIRT: PVR0361922, PVR0362258, PVR0362584, PVR0388249 - IBM SDK, Java Technology Edition Quarterly CPU - Apr 2022 - Includes Oracle April 2022 CPU (minus CVE-2022-21426)	CVE-2022-21496 CVE-2022-21434 CVE-2022-21443 CVE-2022-21299 CVE-2021-35561 CVE-2021-41041
GRD-62342	PSIRT: PVR0359189 - [All] PostgreSQL - CVE-2022-1552 (Publicly disclosed vulnerability)	CVE-2022-1552

CyberArk Version Download

Guardium Version	Bundle	CyberArk Patch Version
v11.0		p1000
	July 2022 bundle and after	p1014
v11.1		p1000
	Aug 2022 bundle and after	p1014

v11.2		p1008
	p275 (Aug 2022 bundle) and after	p1014
v11.3		p1008
	p370 (July 2022 bundle) and after	p1014
v11.4		p1008
	p430 and after	p1014
v11.5		p1014