IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release/ Version	Guardium patch 11.0p277
Name of file:	SqlGuard-11.0p277_Bundle_Oct_26_2022.tgz.enc.sig
MD5SUM	fd86d617e117c48beaf201fea5e564a8
Release	26 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 11.0p200. See release notes for patch v11.0p200.
- The latest health check patch 11.0p9997

Notes:

- This patch restarts the Guardium system.
- Install this patch on all appliances in a top-down manner, starting with the Central Manager, then Aggregators, and then the Collectors.
- Install this patch during the "quiet" time on the appliance.
- If the downloaded package is in .ZIP format, customers are required to extract it outside Guardium appliance before uploading/ installing it.
- **Note: CyberArk customers who are currently on CyberArk patch1008 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

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 file **SqlGuard-11.0p277_Bundle_Oct_26_2022.tgz.enc.sig** (patch 11.0p277) 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.

Bug Fixes

Patch	Issue key	Summary	APAR
11.0p265		Link to patch 11.0p265 on IBM Fix Central (Resolves CVE-2021-45046 and CVE-2021-45105 for Log4j 2.17 in the Guardium system. To resolve Log4j 2.17 in the IBM Spectrum Protect (TSM) client, you must also download and install patch 11.0p1013 by using the following link: patch 11.0p1013)	
11.0p270		Link to patch 11.0p270 on IBM Fix Central	
11.0p275		Link to patch 11.0p275 on IBM Fix Central	
11.0p277	GRD-63513	Patch p370 fails to install in CM with EFI Boot option.	GA18079
	GRD-62550	[v11.0p275]show system service_status doesnt include status for Guardium services cas/gim/stap_upload	
	GRD-62456	[v11.0p275] Couldn't register p275 CM to 3.1.7 GI, error 'certificate signed by unknown authority'	
	GRD-62304	V11.2 | Need Fix for the complete list of Guardium Vulnerabilities identified.	PSIRT
	GRD-62120	v11.4 CyberArk Installation Fails	GA18020
	GRD-61605	[11.2 Bundle] Solar is not running	
	GRD-60733	NOT RECEIVING ALERTS OF TYPE="MAIL" FROM POLICY (TYPE="SYSLOG" are logged fine)	GA18021
	GRD-60386	Vulnerability detected on CyberArk credential provider	GA17923
	GRD-60327	V11.0 MySQL certificate extension request + extended support contract customer.	GA17954
	GRD-59840	11.0p353: Policy export to XACML File crashes GUI	
	GRD-59728	V11.2|V11.3|V11.4 (Regression): Distributed scheduled report does not show data when DR is created using "Guardium Logins" predefined report	
	GRD-59128	CVE-2017-13098 vulnerability on port 16019 for Guardium v10.6	GA18012

	GRD-59091	Running 'store certificate gim client console' with 'r' and 'a' option is not generating keystore for clients	GA17929
	GRD-57807	VA Scan Failing but No Details Indicated (No Privileges With The Grant Option)	GA17911
	GRD-57579	rsyslog cache files and their management	GA17917
	GRD-57197	V11.4[p410]: Non regression: "guard_filetransfer.pl: get transfer method" should be SFTP in guard_filetransfer_log file	
	GRD-54455	EngineID is not Unique for SNMPv3	N/A

Known Limitations

Issue Key	Description
GRD-62968	Insights not supported with v11.2

Security Fixes

Issue key	Summary	Custom field (CVEs)
GRD-62345	PSIRT: PVR0361922, PVR0362258, PVR0362584 - 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
GRD-62342	PSIRT: PVR0359189 - [All] PostgreSQL - CVE-2022-1552 (Publicly disclosed vulnerability)	CVE-2022-1552
GRD-62036	Security Fixes: Multiple Red Hat components need updating	
GRD-61110	PSIRT: PVR0351570 - [All] Apache Struts - CVE-2021-31805 (Publicly disclosed vulnerability)	CVE-2021-31805
GRD-61061	PSIRT: PVR0353709 - [All] Oracle MySQL (Publicly disclosed vulnerability) - Apr 2022 CPU	CVE-2022-21413 CVE-2022-21423 CVE-2022-21482 CVE-2022-21490 CVE-2022-21425 CVE-2022-21460 CVE-2022-21412 CVE-2022-21444

		CVE-2022-21489 CVE-2022-21484 CVE-2022-21462 CVE-2022-21485 CVE-2022-21427 CVE-2022-21478 CVE-2022-21435 CVE-2022-21437 CVE-2022-21417 CVE-2022-21483 CVE-2022-21414 CVE-2022-21454 CVE-2022-21436 CVE-2022-21479 CVE-2022-21415 CVE-2022-21440 CVE-2022-21418 CVE-2022-21452 CVE-2022-2145 CVE-2022-21486
GRD-60930	PSIRT: PVR0338517 - protobuf-java-2.4.1.jar (Publicly disclosed vulnerability found by WhiteSource) - webapps	CVE-2021-22569
GRD-60564	PSIRT: PVR0343484 - [USE THIS] OpenSSL (Publicly disclosed vulnerability)	CVE-2022-0778
GRD-60309	PSIRT: PVR0338428 - jackson-dataformat-cbor-2.9.4.jar (Publicly disclosed vulnerability found by WhiteSource)	CVE-2020-28491
GRD-60283	PSIRT: PVR0344948 - jackson-databind-2.12.6.jar (Publicly disclosed vulnerability found by WhiteSource) - webapps	CVE-2020-36518
GRD-59976	PSIRT: PVR0338445 - junit-4.12.jar (Publicly disclosed vulnerability found by WhiteSource)	CVE-2020-15250
GRD-59953	PSIRT: PVR0338517 - protobuf-java-2.4.1.jar (Publicly disclosed vulnerability found by WhiteSource) - datastreams	CVE-2021-22569 CVE-2020-28491
GRD-59834	PSIRT: PVR0337127 - postgresql-42.0.0.jar (Publicly disclosed vulnerability found by WhiteSource)	CVE-2020-13692 CVE-2022-21724-8.5
GRD-59721	PSIRT: PVR0334551, PVR0336325, PVR0335982 - IBM SDK, Java Technology Edition Quarterly CPU - Jan 2022 - Includes Oracle January 2022 CPU (minus CVE-2022-21299)	CVE-2022-21365 CVE-2022-21360 CVE-2022-21349 CVE-2022-21341 CVE-2022-21340 CVE-2022-21305

		CVE-2022-21294 CVE-2022-21293 CVE-2022-21291 CVE-2022-21248 CVE-2021-35550 CVE-2021-35603
GRD-59571	Security Fix: remove mongodb-org-server from appliances	
GRD-59543	Security Fix: multiple Red Hat components need upgrade	CVE-2020-24489 CVE-2020-24511 CVE-2020-24512 CVE-2020-24513 CVE-2021-25217 CVE-2021-25219 CVE-2021-3472 CVE-2021-31535 CVE-2020-15862 CVE-2020-8625 CVE-2021-26937 CVE-2020-15999 CVE-2021-20305 CVE-2021-20271 CVE-2021-37750 CVE-2021-42574 CVE-2016-5766
GRD-59340	PSIRT: PVR0288118 - [USE THIS] OpenSSL - CVE-2021-3712 (Publicly disclosed vulnerability) - appliance - Dep Delay Exception	CVE-2021-3712
GRD-58848	PSIRT: PVR0328272 - [All] PolicyKit - CVE-2021-4034 (Publicly disclosed vulnerability)	CVE-2021-4034
GRD-58820	PSIRT: PVR0326202, PVR0339413 - [All] PostgreSQL(Publicly disclosed vulnerability)	CVE-2021-23222 CVE-2021-3677
GRD-58089	PSIRT: PVR0316527, PVR0325276 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - jackson-databind-2.10.0.jar	CVE-2020-25649
GRD-58078	PSIRT: PVR0316544 - Using components with Known Vulnerabilities - jsoup-1.12.1.jar	CVE-2021-37714
GRD-58069	PSIRT: PVR0316545 - Using components with known vulnerabilities - kafka-clients-2.5.0.jar - Delay Exception	CVE-2021-38153
GRD-58067	PSIRT: PVR0309383 - Missing Â HSTS Headers on certain endpoint responses	CVE-2012-5627 CVE-2021-3449

GRD-58009	PSIRT: PVR0316519 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - guava-26.0-android.jar	CVE-2020-8908
GRD-58008	PSIRT: PVR0309380 - PEN-TEST: SANS25 - Stored XSS in Discovery Scenarios	CVE-2021-39074
GRD-58007	PSIRT: PVR0309380 - PEN-TEST: SANS25 - Stored XSS in Groups	CVE-2021-39074
GRD-58006	PSIRT: PVR0309380 - PEN-TEST: SANS25 - Stored XSS in Policy Builder interfaces	CVE-2021-39074
GRD-58005	PSIRT: PVR0309380 - PEN-TEST: SANS25 - Unauthenticated stored Cross-Site Scripting in system manager graphs	CVE-2021-39074
GRD-58001	PSIRT: PVR0316537 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - guava-20.0.jar	CVE-2018-10237 CVE-2020-8908
GRD-57993	PSIRT: PVR0309384 - PEN-TEST: Selection of Less-Secure Algorithm During Negotiation in IBM Security Guardium - tls1 and tls1.1 enabed on ort 16019	CVE-2021-39076
GRD-57990	PSIRT: PVR0309378 - Pen Testing 2021 - GimServer (Guard Installation Manager) logs passwords and keys in log file	CVE-2021-39077
GRD-57986	PSIRT: PVR0316535 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - cxf-rt-rs-client-3.1.12.jar	CVE-2018-8039 CVE-2019-12406 CVE-2019-12423 CVE-2020-13954 CVE-2020-1954 CVE-2021-22696 CVE-2021-30468
GRD-57982	PSIRT: PVR0316531 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - cxf-core-3.1.16.jar	CVE-2019-12406 CVE-2019-12423 CVE-2020-13954 CVE-2020-1954 CVE-2021-22696 CVE-2021-30468
GRD-57980	PSIRT: PVR0316533 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium - commons-io-2.4.jar (Solr)	CVE-2021-29425
GRD-57978	PSIRT: PVR0254744 - Pen Testing 2021 - Clear text transmission of passwords by guard_filetransfer.pl	CVE-2021-20385

GRD-57972	PSIRT: PVR0316522 - PEN-TEST: Using components with known vulnerabilities in IBM Security Guardium - kernel	CVE-2016-4658 CVE-2019-11719 CVE-2019-11756 CVE-2019-17006 CVE-2020-6829
GRD-57970	PSIRT: PVR0309382 - Pen Testing 2021 - Admin passwords passed to command line when installing an application	CVE-2021-39078
GRD-57540	PSIRT: PVR0312402 - log4j1 vulnerability (CVE-2021-4104) - UI	CVE-2021-4104

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