IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium patch 10.0p692
Name of file:	SqlGuard-10.0p692_Bundle_May_12_2022.tgz.enc.sig
MD5SUM:	67ffe26b9d0fcd572d152b4ae783f320
Release:	24 May 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: 10.0
- Platform: UNIX/Linux/Windows
- Click “Continue”, then select “Browse for fixes” and click “Continue” again.
- Select “Appliance Patch (GPU and ad hoc)”

Prerequisites:

- Guardium 10.0p600. See patch release notes for 600
- The latest health check patch 10.0p9997

Notes:

- If you are on z/OS, see the known limitations for this patch before you apply it.
- Patch 10.0p692 is an appliance bundle that includes all fixes for 10.6 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

Bug Fixes

Patch	Issue key	Summary	APAR
10.0p684		Link to patch 10.0p684 in Fix Central	
10.0p685		Link to patch 10.0p685 in Fix Central	
10.0p690		Link to patch 10.0p690 in Fix Central	
10.0p692	GRD-58428	Data restore failure	GA17916
	GRD-57579	rsyslog cache files and their management	GA17917
	GRD-51104	CVE-2004-2761 ssl certificate signed using weak hashing algorithm on port 8586	GA17608

Known Limitations

Issue Key	Description
GRD-60377	Exporting reports in PDF and full printable view does not work for multi-language support.
GRD-60259	If Sniffer patch 11.0p4039 is installed, installing patch 11.0p430 will cause errors in multi-byte representation. **Resolution:** available in an upcoming Sniffer patch.

Security Fixes

Issue key	Summary	CVEs
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-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-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-57736	PSIRT: PVR0316546 - PEN-TEST: Using components with known vulnerabilities in IBM Security Guardium - libfb303 - Delay Exception	CVE-2016-5397 CVE-2018-11798 CVE-2018-1320 CVE-2019-0205 CVE-2019-0210 CVE-2020-13949