IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium 11.5
Patch description:	Guardium patch 11.0p511
Name of file:	SqlGuard-11.0p511.tgz.enc.sig
MD5SUM:	5fd1a0783ed324c8ddfdc9758fe5aec8

CAS Builds required with Patch 511:

Guardium_11.5.0.0_CAS_HPUX_r113541.zip
Guardium_11.5.0.0_CAS_Solaris_r113541.zip
Guardium_11.5.0.0_CAS_AIX_r113541.zip
Guardium_11.5.0.0_CAS_RedHat_r113541.zip
Guardium_11.5.0.0_CAS_Suse_r113541.zip
Guardium_11.5.0.0_CAS_zLinux_r113541.zip
Guardium_11.5.0.0_CAS_Ubuntu_r113541.zip
Guardium_11.5.0.0_CAS_Debian_r113541.zip

Special DPS required with Patch 511:

Guardium_V11_Quarterly_DPS_2022_Q4_20221230.enc

Date: 21 December 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: 11.5
- Platform: UNIX/Linux/Windows
- Click “Continue”, then select “Browse for fixes” and click “Continue” again.
- Select “Appliance Patch (GPU and ad hoc)”

Prerequisites:

- Guardium appliance bundle 11.0p510
- The latest health check patch 11.0p9997

Notes:

- Patch 11.0p511 is an appliance bundle that includes all fixes for 11.5 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.
- The DPS file named: Guardium_V11_Quarterly_DPS_2022_Q4_20221230.enc needs to be applied after applying Patch 511, if it is installed before the upcoming Q1 Feb 2023 DPS. If Patch 511 is installed after the Q1 Feb 2023 DPS, then applying the latest DPS is sufficient, as it is cumulative.

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

New features

Vulnerability Assessment now supports the following data sources and CIS benchmarks:

- Apache Cassandra datasource
- Percona MySQL datasource
- MongoDB 4.0 and MongoDB 5.0 Benchmark v1.0.0
- Oracle MySQL Enterprise Edition 8.0 Benchmark v1.2.0.

For datasource configuration information, see Apache Cassandra, MySQL, and Percona MySQL.

For supported versions, see: https://www.ibm.com/support/pages/node/6613461.

Security Fixes

Issue key	Summary	CVEs
GRD-53428	CIS Benchmark for DB - MongoDB 4.0 and Mongov5.0 Benchmark v1.0.0	
GRD-53427	CIS Benchmark for DB - Oracle MySQL Enterprise Edition 8.0 Benchmark v1.2.0	
GRD-58861	VA Support for Apache Cassandra	
GRD-59371	VA Support for Percona MySQL	
GRD-64670	Investigate Snowflake issues from 11.5 beta customer	

GRD-64420	Unexpected error while viewing Security Policy Ad hoc analysis results	
GRD-66134	Fix the resume test list problem	
GRD-65693	Test ID 2340 fails because it checks the wrong system parameter QPWDRQDDIF instead of QPWDPOSDIF	
GRD-65434	PSIRT: PVR0396012 - commons-text-1.9.jar (Publicly disclosed vulnerability found by Mend)	CVE-2022-42889