IBM Security Guardium Patch Release Notes

Product:	IBM Security Guardium
Release:	Guardium 10.6
Patch description:	Guardium patch 10.0p1025
Name of file:	SqlGuard-10.0p1025_Bundle_Jul_20_2023.tgz.enc.sig
MD5SUM:	848ce200e36d843e15018f3f6433e4c4
Date:	18 August 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: 10.0
- Platform: UNIX/Linux/Windows
- Click "Continue", then select "Browse for fixes" and click "Continue" again.
- Select "Appliance Patch (GPU and ad hoc)"

Prerequisite:

- Guardium 10.6- see release notes for version 10.0p600
- The latest health check patch 10.0p9997

Notes:

- Patch 10.0p1025 is an appliance bundle that includes all fixes for 10.6 except sniffer fixes.
- This patch restarts the 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-72303	You can now provide different levels of CAS server authentication support, from a non-secure connection to a secure connection with a signed certificate. See here for more information. The supported versions for this change are as follows: • UNIX/Linux: 10.6.1.1_r115211 • Windows: V10.6.0.429

Bug Fixes

Patch	Issue key	Summary	APAR
10.0p1016		Link to previous patch release note in Fix Central	
10.0p1025	GRD-70373	Tomcat failing with OutOfMemoryError and generating Java coredumps	GA18308
	GRD-69136	Data Archive to Amazon S3 failing after applying patch p694	GA18307
	GRD-69066	Updates to accessmgr and admin passwords on the CM are not updated on the Managed Units after installing patches 694 or 699	GA18269
	GRD-65632	QID 38738 vulnerability reoccurs after restart	GA18279

Security Fixes

Issue key	Summary	CVEs
GRD-69998	PSIRT: PVR0405170 - Cross-Site Scripting in IBM Security Guardium	CVE-2022-43909
GRD-69994	PSIRT: PVR0431620, PVR0431924 - IBM SDK, Java Technology Edition Quarterly CPU - Jan 2023 - Includes Oracle January 2023 CPU and IBM Java XML vulnerability	CVE-2023-21830 CVE-2023-21843 CVE-2022-21426
GRD-68973	PSIRT: PVR0316540 - Pen Testing 2021 - Using components with known vulnerabilities in IBM Security Guardium -	CVE-2020-13956

	httpclient-4.5.10.jar - SOLR - Dep Delay Exception	
GRD-66016	PSIRT: PVR0405168 - Pen Testing 2022 - SANS25 -Â OS Command Injection - System Backup UI	CVE-2022-43907
GRD-66027	PSIRT: PVR0405164 - Pen Testing 2022 - Hazardous Input Validation - refresh rate field	
GRD-66024	PSIRT: PVR0405169 - Pen Testing 2022 - Improper Authentication - broken access control	CVE-2022-43908
GRD-66005	PSIRT: PVR0405165 - Pen Testing 2022 - SANS25 - Improper Restriction of Excessive Authentication Attempts	