Privilege Management for Unix and Linux 22.3 Release Notes

December 16, 2022

Issue Resolved in 22.3.0-12 (Replacing 22.3.0-11):

- The field "replay_link" in Solr schema that was removed in version 22.3.0-11 is now restored in version 22.3.0-12. BIUL uses this link to find the logserver on which the iologs are located.

New Features and Enhancements:

RNS

- When adding, promoting, and deleting a host, contents of service database is synced across secondary RNS servers and service cache of all servers are updated.
- Service cache database on REST enabled remote host can be now force updated from RNS primary server using the command **pbdbutil --scache -R --all**.
- Added a new option **pbdbutil --svc -d --remove** to completely remove a host entry from services database.
- Add an option to **pbdbutil** to update a host in the service database.

Dbsync

- On-demand database sync through **pbdbutil --dbsync -R <svc>** option now syncs databases, CFG files and REST keys only for the requested service group.
- Changed config database **pb.db** schema to improve the performance. BLOB column **data** is moved to a separate table.
- Added a new **pbdbutil --cfg –reinit** option to create new or upgrade existing **pb.db**.
- Dbsync of **cfgfiles** synchronizes **created** date, file permissions, and file tag for all versions of **cfgfile** from primary server to the secondary servers.
- You can now force synchronize all versions of CFG files from primary to secondary using **pbdbutil --dbsync -R <svc> --force** option.

Logserver/REST Services Failover Hardening

- PMUL currently has the ability to specify several logservers. When the initial connection is made to pblogd, if a logserver does not respond within logserverdelay milliseconds, a connection is attempted to the next logserver in the list.

  In v22.3.0, we have added another level of failover, when the connected log server experiences a failure after that connection is established. This new functionality takes place only in the rare case where a connection and validation are successful, but ultimately logging the event fails (due to lack of space, or other reasons).

  Additionally, if the REST services on the logserver fail, after connection to the services is established, PMUL will failover to the next logserver to connect to REST services on that host.

Policy Function "setkeystrokeaction" Custom Message

- The PMUL policy function **setkeystrokeaction** allows the policy to specify keystroke patterns that are not allowed and thus terminate the secured task. The secured task is killed, and the end user sees: *3005 Request ended unexpectedly*, followed by the normal shell prompt, but not aligned.

  This feature adds an optional message argument to the function and aligns the output, when that argument is specified, and the **action** parameter is **reject**. Without the new argument, PMUL behaves as it has in the past.

  Current syntax:

  setkeystrokeaction(pattern, patterntype, action);

  New syntax:

  setkeystrokeaction(pattern, patterntype, action [, message]);

  This is a change to the policy language; therefore, the policy server must be at version 22.3.0 in order for the policy to parse without a syntax error. The submithost and runhost components must also be on version 22.3.0 for the new feature to work. If the optional message is specified, but the submithost or runhost are on a previous version, the feature will *silently* fall back to the old behavior.

REST Services/pbdbutil/Message Router

- Added options to **pbdbutil** to read a WQ file and display information on the file.
- Added memory leak protection in the WQ processing.
- The status of each license record in the license WQ file is now updated properly, therefore already processed license records are not reprocessed.
- The output of **pbdbutil --info –msg –level=2** now displays *semaphore_count*, *next_empty*, *next_full fields*.
- **pbdbutil –info –msg** previously always displayed *0* for replies in the **authenticate** section. It now shows the number of authentications for replies.

Miscellaneous

- The output of **pbdbutil –lic –wq** now displays more details like the number of records processede and the last batch number.
- The permissions of the **writequeuepath** directory and WQ files are now checked to ensure they are secure.
- The **replace()** function in the policy language now properly supports insertion of lists in lists.
- The output of **ps -ef** for PMUL processes: added the following text in the *ps* information to **pblogd** to show more about the state of **pblogd**: accept, finish, reject, keystroke, open log, close log, write I/O log, mktemp, reconnect.
- Issues related to the use of the hostname of the host is used on the **localhost** line (127.0.0.1 or ::1) in **/etc/hosts**, in RNS and licensing are now resolved.
- A new REST call was added (**REST/v2/settings/verify**) to verify the values of each setting and return an error for each incorrect value.
- Enhanced the **/settings** REST call to add errors to each of the settings in error.
- Resolved issue in which **pbuninstall** on Solaris 10 was failing with: *./pbuninstall: test: argument expected*.
- Other minor issues.

Issues Resolved:

RNS

- Deleting a secondary server now properly cleans up its entry from primary server's dbsync list for related service groups.
- Service cache list is polished to list only appropriate entries for each host: it lists all the servers of any service group and service groups for which the host is a client and does not list other client-only hosts.
- Added database versioning for service database and service cache database.
- Deleting a host now deletes host entries from service cache database of non-RNS servers/clients.
- The hostname **cn** attribute can be now updated using the command **pbdbutil --svc -u**.

Dbsync

- RNS: resolved misleading error displayed during DB sync for files marked as deleted in **pb.db**.
- RNS/dbsync: cfgfiles: resolved issue in which setting a file for autosync for more than one service group resulted in NOT user friendly svc field display.
- RNS:presolved issue in which promotion of Sudo Policy Server along with Registry Server causeed HTTP error/status 4037 - 4037.02.
- Resolved multiple issues in updating **lasttid** for each host, service group in dbsync database.
- RNS/dbsync: resolved issue in which **pbdbutil --dbsync -R** resulted in an error when executed after a **promote** and before **dbsyncrefresh time**.

REST Services/pbdbutil/Message Router

- WQ files were taking a long time to be processed, consuming CPU and as well as the read timeout values were over several hours. They are now processed immediately.
- An infinite loop during processing of events by message router, when the eventlog was insecure, was corrected.

Notes:

IMPORTANT!

A high severity vulnerability was discovered in the sudomgr component of BeyondTrust's Privilege Management for Linux (PMUL) that could allow an attacker to elevate their privileges on Linux systems.

*It was discovered that SudoManager (formerly known as **pbsudo**), a component of PMUL, is affected by CVE-2023-22809. This vulnerability within sudoedit mishandles arguments passed in as user-provided environment variables, allowing a local attacker to append arbitrary entries to the list of files to process. Successful exploitation can lead to privilege escalation on Linux systems.*

Affected Versions

Product	*Version*
pbsudo	*All versions*
sudomgr	*22.2.0 through 22.3.0-12*

Fixed Versions

Product	*Version*
pbsudo	*Upgrade to sudomgr 22.3.1-01*
sudomgr	*22.3.1-01*

Mitigation

A patch is available for download and should be applied to vulnerable SudoManager systems. We urge customers still using pbsudo to upgrade to sudomgr 22.3.1-01 or later.

References

NVD - CVE-2023-22809 (nist.gov) at https://nvd.nist.gov/vuln/detail/CVE-2023-22809

CVE - CVE-2023-22809 (mitre.org) at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22809

- Upgraded Curl from 7.83.0 to 7.85.0.
- Upgraded SQLite from 3.36.0 to 3.39.4.
- Integration with BeyondInsight is now deprecated in favor of BIUL and ElasticSearch. We have also officially removed **pbguid** in v22.3.0.
- Added support for RHEL 9.
- Removed support for SUSE 11.
- Removed support for Oracle Linux on SPARC.