



**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE
REPORT
ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0

Maintenance Report Number:

CCEVS-VR-VID110691-2018a

Date of Activity:

27 July 2018

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3.0, September 12, 2016

NIAP Policy #12 “Acceptance Requirements of a product for NIAP Evaluation.” March 20, 2013

Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0 Security Target Version 1.1 1 June 1, 2018

BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0 Impact Analysis Report Version 1.3 July 27, 2018

Affected Developer Evidence:

BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0 Security Target Version 1.1 1 June 1, 2018

PowerBroker for Unix & Linux Common Criteria – Supplementary Guide (Updated 07-10-2018)

BeyondTrust PowerBroker UNIX + Linux Edition V9.1 Common Criteria Test Report and Procedures, Version 1.0, May 25, 2016

PowerBroker for Unix & Linux System Administration Guide v10.0

PowerBroker for Unix & Linux Installation Guide v10.0

Description of Changes:

The BeyondTrust PowerBroker ® UNIX® + Linux® Edition software was updated from version v9.1 to version v10.0. The software updates included new non-security relevant features and bug fixes. The software updates include:

- Advanced Control & Audit (ACA) – optional policy configuration
- Solr Host - optional component used for IOlog Indexing
- PowerBroker Management Console - A free utility provided by BeyondTrust
- File Integrity Monitoring - an optional component
- Registry Name Services - an optional component for people not want to use DNS
- Sudo Client - Separately sold and licensed product
- Advanced Keystroke Actions - Separately sold and licensed product

None of these software components are required for the evaluated configuration, and none were included in the original evaluation or the IAR.

Three updates have been identified as affecting the TOE from the previous evaluation. These are minor changes that do not affect any of the SFRs or claimed security functionality. The Security Target and the CC Guidance have been updated to reflect these changes as appropriate. These updates were changes to:

- Centralized Licensing - this update resulted in the TOE version changing from v9.x to v10.0
- Installation default file location - on a new install, the default policy directory is changed from /etc to /opt/pbul/policies
- PowerBroker for Unix & Linux GUI - the GUI is now available as a separate download from the BeyondTrust customer portal. The PowerBroker for Unix & Linux GUI (pbguid) provides all the functionality identified in the ST; the only difference is the download method

The table below summarizes the product updates by version. These changes are not considered to be security relevant and do not affect any of the claimed security functionality or affect any of the SFRs identified in the ST.

Product Updates by Version	Significant Example Updates
10.0.1	<ul style="list-style-type: none"> • Splunk Integration
10.0.0	<ul style="list-style-type: none"> • Centralized licensing database with component based licensing options • Integration with PowerBroker Management Console (PBSCM) V6
9.4.5-10	<ul style="list-style-type: none"> • File Integrity Monitoring Updates • REST API • Client-based REST Services
9.4.4-10	<ul style="list-style-type: none"> • Advanced Keystroke Action • Role-based policy improvements
9.4.3-18	<ul style="list-style-type: none"> • PowerBroker for Unix & Linux GUI is now available as a separate download from the BeyondTrust customer portal • Advanced Control & Audit (ACA) enhancements • File Integrity Monitoring (FIM) enhancements
9.4.1-03 (replacing 9.4.0-18)	<ul style="list-style-type: none"> • ACA enhancement
9.4.0-18	<ul style="list-style-type: none"> • File Integrity Monitoring (FIM) • Registry Name Service is a service • Database Synchronization
9.3.0-07	<ul style="list-style-type: none"> • New keyword (randomizelogservers) added
9.2.0-08	<ul style="list-style-type: none"> • Support for DNS names longer than 63 characters

Bug fixes are identified in the IAR for all the version listed in the table above. The assessment of the all the bug fixes has been classified as “minor”. The assessment specifies that either 1) the bug fixes do not affect any of the SFRs or claimed security functionality, 2) none of the audit records identified in the ST are affected by the enhancement, or 3) the software component was not included in the evaluated configuration.

Assurance Continuity Maintenance Report:

- There have been feature updates to the TOE since the previous Validation report of August 30, 2016, and the previous Impact Analysis Report submission in April 2018. These changes are described above.
- The Impact Analysis Report specifies that no functionality, as defined in the SFRs, was impacted by the software update and bug fixes of the BeyondTrust PowerBroker Unix+Linux Edition v10.0.
- The functionality of the BeyondTrust PowerBroker Unix+Linux Edition v10.0 remains the same as prior evaluated version. The product updates and bug fixes do not affect the security functional requirements identified in the Security Target.
- For this Assurance Continuity, the change consists of making the following firmware minor version updates:
 - From: BeyondTrust PowerBroker ® UNIX® + Linux® Edition V9.1
 - To: BeyondTrust PowerBroker ® UNIX® + Linux® Edition V10.0
- BeyondTrust added numerous product updates. As identified above, most of product updates are optional features and were not included in the original evaluation. They are not claimed in the present IAR and the evaluated configuration remains the same with the three exceptions for Centralized Licensing, Installation default file location, and PowerBroker for Unix & Linux GUI, as detailed above in the description of changes section.
- The Impact Analysis Report vulnerability analysis describe the changes and specify why the changes are minor and do not impact the security functionality of the product.
- The changes to the Security Target and Common Criteria Guidance Document reflect the updates described above.

Description of Regression Testing:

BeyondTrust performs full regression testing on all released product version updates. The regression testing is performed because of new product updates and bug fixes. The proprietary BeyondTrust QA Test Strategy – PowerBroker for UNIX / Linux document identifies the functional and system testing performed for each product release. Testing is performed on all supported operating system platforms, including the supported operating system platforms and hardware architectures identified in the Security Target Section 2.2.1. The regression testing verified that the product performed correctly after the described changes.

Vulnerability Assessment:

The evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability. The vulnerability assessment was conducted on June 29, 2018, and included the search terms BeyondTrust, PowerBroker, Enterprise Security Management, Controlled Access, Policy Management, Privilege Elevation, Spectre, and Meltdown.

Vendor Conclusion:

The specific changes made to the BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0 do not affect the security claims in the BeyondTrust PowerBroker UNIX® + Linux® Edition V10.0 Security Target.

The updates result in no changes to SFRs, Security Functions, Assumptions or Objectives, Assurance Documents, or TOE Environment and therefore are a minor change. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the updates.

Validation Team Conclusion:

The Validation team has reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of this product.