CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR:

Brocade Communications Systems, Inc. Directors and Switches, w/FabricOS Version 7.2.0a

Maintenance Report Number: CCEVS-VR-VID10376-2014

Date of Activity: 29 January 2014

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

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

*Impact Analysis Report for Brocade Communications Systems, Inc. Dir*ectors and Switches, w/FOS 7.2.0a, Version 0.1

Affected Evidence:

Brocade Directors and Switches Security Target, Version 3.0, February 12, 2013

Brocade Fabric OS v7.0.0b1 Release Notes v1.0

Fabric OS Administrators Guide Supporting Fabric OS, v7.1.0, 53-1002745-01, 14 December 2012

Fabric OS Command Reference Supporting Fabric OS, v7.10, 53-1002746-01, 14 December 2012

Updated Developer Evidence:

Brocade Directors and Switches Security Target, Version 3.1, November 26, 2013

Fabric OS Administrator’s Guide Supporting Fabric OS 7.2.0, 53-1002920-01, 26 July 2013

Fabric OS Command Reference Supporting Fabric OS 7.2.0, 53-1002921-01, 26 July 2013

Brocade Fabric OS v7.2.0a Release Notes v1.0, September 9, 2013

Assurance Continuity Maintenance Report:

Gossamer Laboratories CCTL, on behalf of Brocade Communications Systems Inc., submitted an Impact Analysis Report to CCEVS for approval on November 26, 2013. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

Brocade Communication has revised the OS supporting their hardware appliances from Fabric OS version 7.1 to Fabric OS version 7.2.0a. The OS update represents changes made to the TOE to include the changes represented in the Assurance Continuity Maintenance Report for Brocade Directors and Switches, Software FabricOS Version 7.1, CCEVS-ACMR-10376-2013:

- Support for new appliances; embedded switch models 5431, 6547 and M6505.
- The addition of a monitoring and alerting suite (MAPS),
- An administrative tool, “Flow Vision” that provides visibility into application flows within the fabric.
- Fibre Channel Routing enhancements for link selection between FCR edge fabrics and the FCR backbone fabric.
- Fibre Channel IP enhancements to the FCIP Tunnel failover configuration.
- ClearLink Diagnostics - D_Port functional enhancements to test result reporting as well as the addition of dynamic port switching to the 16G HBA and 16G switches.
- Access Gateway Enhancements D_Port Diagnostics for SFP and cable health, and the detection and prevention of duplicate Port World Wide Names.
- Encryption Platform enhancements wherein the encryption platforms can now interact with two more corporate level storage solutions and the Thales e-Security Key Authority.
- Fibre Channel Connection enhancements that include the addition of error codes to the protocol.
- FOS v7.2 allows 10G speed configurations on all ports of a 16G FC blade and 16G switch (6510, 6520 only). It also provides more flexibility to enable encryption/compression on 10G ports.
- Pre-FOS v7.2 limited 10G FC support to only the first 8 ports of a 16G switch or a 16G blade. This also limited the ability to enable encryption/compression to only two of those first 8 ports due to restrictions on the number of ports supported per ASIC. By removing this restriction, FOS v7.2 allows users to enable more 10G FC ports for encryption and compression by spreading them across multiple ASICs.
- FOS v7.2 allows buffer credit assignment even for “normal distance” (regular) E_ports
- The portCfgEportCredits CLI introduced in FOS v7.2 allows users to perform fine grained performance tuning on normal E_ports by allowing users to specify buffer credits.
- In FOS v7.2, the portaddess CLI has been enhanced to display an address as user bound when a user has explicitly bound an address to a port.
- FOS v7.2 introduces a new CLI “creditrecovmode” to configure backend link credit loss recovery options. This change simplifies the bottleneckmon CLI.

- FOS v7.2 allows users to provide a reason string when disabling a port via portdisable or portcfgpersistentdisable CLIs – helps to track the user intention for disabling a particular port.
- FOS v7.2 introduces new RASlogs (FSPF-1013, FSPF-1014) and new CLI outputs in fabricshow and topologyshow to indicate when the maximum paths (16) to a remote domain are exceeded.
- Maintenance fixes to address software bugs.

Vendor Conclusion: "The changes consist of the addition of three new embedded appliances and replacing the Fabric OS 7.1 with Fabric OS 7.2.0a. The three additional hardware models provide the same security functionality as the previously evaluated models. They simply provide additional performance options.

The Fabric OS 7.2.0a was revised to add a number of features, and fix a number of bugs. These changes are primarily related to changes in network protocol and service improvements and as indicated above none is related to the security claims in the evaluated ST.

The evaluation evidence consists of the Security Target, hardware manuals, administrative guidance, design documents, life cycle documents, and test evidence. The Security Target was revised to reflect the new embedded products and the change in Fabric OS version. The hardware manuals are unchanged, except that a new hardware manual has been identified for the new appliances. The release notes have been updated to reflect the new Fabric OS version, but otherwise all guidance includes the content evaluated in the previous versions."

Validation Team Conclusion: The changes to the TOE are confined to software. The vendor claims that testing of the specific changes and a set of regression testing was conducted. Those test logs and supporting evidence were not provided in the IAR package. The validation team concurs that most changes were functional in nature; however the validation team notes the following:

- The MAPS suite is part of the OS, however it requires the purchase of additional license(s) before it is activated.
- The MAPS suite provides functionality and features that are not covered in the original or updated ST, and as such the use of MAPS is outside the scope of the evaluation and its use places the product in an unevaluated configuration. No claims can be made as to its effectiveness or its security impact.
- Flow Vision is part of the operating system but requires additional licensing to activate. Flow Vision was not evaluated, and no claims can be made as to its effectiveness or its security impact.
- PWWN – Port World Wide Naming. The use of Port World Wide Naming is outside of the evaluated configuration.
- Encryption platform enhancements. The enhancements allow for interaction with additional vendor devices as well as an additional Key management device (Thales e-Security) that is outside the TOE. The validation team is of the opinion that the change is security relevant, but could be considered a minor change.
- The use of Fibre Connection (FICON) is outside the scope of the original evaluated configuration. No claims can be made as to the effectiveness or security implications of its use.

The validators reviewed the changes and concur that the changes should be should be classified as minor and that certificate maintenance is the correct path for assurance continuity. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.