National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Hewlett Packard Enterprise
153 Taylor Street
Littleton, MA 01460-1407

Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules

Report Number: CCEVS-VR-10660-2016
Dated: February 17, 2016
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

El Segundo, CA
The Aerospace Corporation

Jay Vora

Annapolis Junction, MD
The MITRE Corporation

Common Criteria Testing Laboratory

Chris Keenan

Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules solution provided by Hewlett Packard Enterprise. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in February 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile for Network Devices, version 1.1, 8 June 2012 with Errata #3.

The Target of Evaluation (TOE) is Hewlett Packard Enterprise (HPE)[1] Moonshot-180XGc, 45XGc, 45Gc Switch Modules. The Moonshot Switches are switch appliances that provide network connectivity for the following: Cloud computing, service providers, Web2.0, health care, Universities, Government agencies and for use in HPE enclosures.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units, assurance activities, and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and

[1] Note: On November 1, 2015, Hewlett-Packard became two separate companies: Hewlett Packard Enterprise and HP Inc. The network products are part of the new Hewlett Packard Enterprise. The former HP network switches and routers are undergoing product rebranding. The rebranding is not complete in the documentation and on the websites. The TOE maybe referred to with the suffix "HP", "HP FlexFabric", "HPE" or "HPE FlexFabric". For the purpose of this evaluation, these name variations are used interchangeably and refer to the same product.

the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Network Devices, version 1.1, 8 June 2012 (NDPP) (including the optional SSH and IPsec requirements) with Errata #3
ST:	Hewlett Packard Enterprise Moonshot 180XGc, 45XGc, 45Gc Switch Modules (NDPP11e3) Security Target, Version 0.3, February 5, 2016
Evaluation Technical Report	Evaluation Technical Report for Hewlett Packard Enterprise Moonshot 180XGc, 45XGc, 45Gc Switch Modules, Version 1.2, February 15, 2016

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 conformant
Sponsor	Hewlett Packard Enterprise
Developer	Hewlett Packard Enterprise
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Daniel Faigin The Aerospace Corporation Jay Vora The MITRE Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.[2]

The Target of Evaluation (TOE) is Hewlett Packard Enterprise (HPE) Moonshot-180XGc, 45XGc, 45Gc Switch Modules. The Moonshot Switches are switch appliances that provide network connectivity for the following: Cloud computing, service providers, Web2.0, health care, Universities, Government agencies and for use in HPE enclosures. The Moonshot Switches include the HPE Comware V7.1 network operating system, which delivers enterprise grade resiliency and is designed for data center convergence with full support for IEEE Data Center Bridging (DCB) for lossless Ethernet, and Fibre Channel over Ethernet (FCoE) protocols. The switches support IETF industry standard TRILL (Transparent Interconnection of Lots of Links) that enables loop free large Layer 2 networks with multi-path support. The switch provides Intelligent Resilient Framework (IRF) which enables multiple switches to be virtualized and managed as a single entity with HPE's Intelligent Management Center (IMC). The IMC is not within the scope of the evaluation. Management of the IRF group can and should occur via any of the IRF group members by an authorized administrator using the CLI (Command Line Interface).

In the evaluated configuration, the switches can be deployed as a single switch device or alternately as a group of up to four devices connected using the HPE Intelligent Resilient Framework (IRF) technology to effectively form a logical switch device. The IRF technology requires that devices be directly connected to one another using an IRF stack using one or more dedicated Ethernet connections that are used to coordinate the overall logical switch configuration and also to forward applicable network traffic as necessary between attached devices. The IRF technology does not require that switches be co-located,

[2] This section may describe capabilities that were not covered by the evaluation. Consult Section 9.8 for the clarification of scope.

but can be attached using standard LACP (Link Aggregation Control Protocol) for automatic load balancing and high availability. Note that the IRF connections are not secured (e.g., using encryption) by the TOE, so the IRF group members must be collocated and the IRF connections need to be as protected as the IRF group devices themselves.

The Moonshot Switches support uplink modules and plug-in modules, which provide additional functionality (e.g., various numbers and types of network connection ports). All of the available plug-in modules are included in the evaluated configuration.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules. The software on all models is Comware V7.1. Each Module can optionally use any of the following Uplink Modules since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HPE Moonshot–4QSFP+ Uplink Module
- HPE Moonshot-16SFP+ Uplink Module
- HPE Moonshot-6SFP+ Uplink Module

3.2 TOE Architecture

The HPE Moonshot-180XGc, 45XGc, 45Gc Switch Modules comprising the TOE includes a common software code base, called Comware. Comware is special purpose appliance system software that implements a wide array of networking technology, including: IPv4 (Internet Protocol Version 4), dual-stacks, a data link layer, layer 2 and 3 routing, Ethernet switching, Virtual Local Area Networks (VLANs, Intelligent Resilient Framework (IRF) routing, Quality of Service (QoS), etc. The evaluated version of Comware is V7.1. It should be noted that Comware runs on a variety of underlying architectures including VxWorks, Linux, pSOS and Windows; however, the only underlying architecture found in the evaluated configuration is Linux.

Comware V7.1 implements full modularization and multi-process applications, as well as providing the following:

- *Full modularization* — Comware V7.1 brings improvements in system availability, virtualization, multi-core multi-CPU applications, distributed computing, and dynamic loading and upgrading.
- *Openness* — Comware V7.1 is a generic, open system based on Linux.
- *Improved operations* — Comware V7.1 improves some detailed operations. For example, it uses preemptive scheduling to improve real-time performance.

Comware V7.1 optimizes the following functions:

- *Virtualization* — Supports N:1 virtualization.
- *In-Service Software Upgrade (ISSU)* — Supports ISSU for line cards.
- *Auxiliary CPU and Open Application Architecture (OAA)* — Improve scalability for devices.

Comware V7.1 comprises four planes: management plane, control plane, data plane, and infrastructure plane. Each is summarized below:

- *Infrastructure plane* – The infrastructure plane provides basic Linux services and Comware support functions. Basic Linux services comprise basic Linux functions, C language library functions, data structure operations, and standard algorithms. Comware support functions provide software and service infrastructures for Comware processes, including all basic functions.
- *Data plane* – The data plane provides data forwarding for local packets and received IPv4 packets at different layers
- *Control plane* – The control plane comprises all routing, signaling, and control protocols, such as Multiprotocol Label Switching (MPLS), Open Shortest Path First (OSPF), and security control protocols. It generates forwarding tables for the data plane.
- *Management plane* – The management plane provides a management interface for administrators and operators to configure, monitor, and manage Comware V7.1. The management interface comprises a CLI accessed using Secure Shell (SSH).

From a security perspective, the TOE implements NIST-validated cryptographic algorithms that support the IPsec and SSH protocols as well as digital signature services that support the secure update capabilities of the TOE. Otherwise, the TOE implements a wide range of network switching protocols and functions.

3.3 Physical Boundaries

A TOE device (HPE Moonshot-180XGc, 45XGc, 45Gc Switch Modules) is a modular switch appliance with a fixed number of ports and modular uplink module.

The TOE can be configured to rely on and use a number of other components in its operational environment.

- *Syslog server* – The Syslog server receives audit records when the TOE is configured to deliver them to an external log server.
- *RADIUS and TACACS+ servers* – The TOE can be configured to use external authentication servers.
- *Management Workstation* – The TOE supports CLI access and as such an administrator would need an SSHv2 client to use the administrative interface.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security Management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to a designated syslog server.

4.2 Cryptographic support

The TOE includes NIST-validated cryptographic mechanisms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols, including IPsec and SSHv2. Note that in the evaluated configuration, the TOE must be configured in FIPS mode, to ensure that CAVP-tested functions are used.

Algorithm	CAVP Cert. #
AES	#3855
RSA	#1969
ECDSA	#834
SHA	#3177
DRBG	#1094
HMAC	#2503
ECC Key Pair Generation	#738

4.3 User data protection

The TOE supports a wide variety of network access control functions. While implementing its network access control functions, the TOE is carefully designed to ensure that it doesn't inadvertently reuse network or management data. This is accomplished primarily by clearing and zero-padding of memory structures and packet buffers when allocated.

4.4 Identification and authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console and a network accessible interface (SSHv2) for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of trusted RADIUS and TACACS+ servers in the operational environment to support, for example, centralized user administration.

4.5 Security management

The TOE provides Command Line (CLI) commands (locally via a serial console or remotely via SSH) to access the available functions to manage the TOE security functions and network access control functions. Security management commands are limited to authorized users (i.e., administrators) only after they have been correctly identified and authenticated. The security management functions are controlled through the use of Admin Roles that can be assigned to TOE users.

4.6 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. The TOE uses a clock managed by the OS for reliable time clock information that the TOE uses (e.g., for log accountability).

The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of a Syslog server or authentication servers in the operational environment, the communication between the TOE and the operational environment component is protected using encryption.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.7 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.8 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. Using SSHv2, both integrity and disclosure protection is ensured. The TOE protects communication with network peers, such as a log server, and authentication servers (RADIUS and TACACS+) using IPsec connections to prevent unintended disclosure or modification of logs.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP). That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Preparative Procedures for CC NDPP Evaluated HPE Moonshot-180XGc, 45Gc and 45XGc Switch Module based on Comware V7.1*, Version 1.01, HP Enterprise. February 9, 2016
- *Command Reference for CC Supplement*, v 1.06, HP Enterprise. February 9, 2016
- *Configuration Guide for CC Supplement*, v 1.6, HP Enterprise. February 9, 2016
- *Comware V7 Platform System Log Messages*, v 1.00, HP Enterprise, December 2, 2015

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the *Detailed Test Report for the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules*, Version 0.2, February 5, 2016.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the *Preparative Procedures for CC NDPP Evaluated HPE Moonshot-180XGc, 45Gc and 45XGc Switch Module based on Comware V7.1*, Version 1.01, February 9, 2016 document and ran the tests specified in the NDPP including the optional SSH and IPsec tests. The assurance activities were addressed within the *Assurance Activity Report for HPE Moonshot-180XGc, 45XGc, 45Gc Switch Modules*, Version 0.3, 02/15/2016.

8 Evaluated Configuration

The evaluated configuration consists of the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules. The software on all models is Comware V7.1. Each Module can optionally use any of the following Uplink Modules since they do not affect any of the claimed security functions but rather serve to extend available network connectivity:

- HPE Moonshot–4QSFP+ Uplink Module
- HPE Moonshot-16SFP+ Uplink Module
- HPE Moonshot-6SFP+ Uplink Module

To use the product in the evaluated configuration, the product must be configured as specified in *Preparative Procedures for CC NDPP Evaluated HPE Moonshot-180XGc, 45Gc and 45XGc Switch Module based on Comware V7.1*, Version 1.01, February 9, 2016.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all work units and assurance activities received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 4 and CEM Version 3.1 Revision 4. The evaluation determined the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules to be Part 2 Extended, and Part 3 Conformant.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Hewlett Packard Enterprise Moonshot-180XGc, 45XGc, 45Gc Switch Modules that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDPP related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC_OPE.1 and ALC_CMS.1 CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA_VAN.1 CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9.8 Clarifications of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the NDPP. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

10 Validator Comments/Recommendations

The validators have no further comments about the evaluation results

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Hewlett Packard Enterprise Moonshot 180XGc, 45XGc, 45Gc Switch Modules (NDPP11e3) Security Target*, Version 0.3, February 5, 2016.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4*, September 2012.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 4, September 2012.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 4, September 2102.

[4] *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (with Errata #3)

[5] *Hewlett Packard Enterprise Moonshot 180XGc, 45XGc, 45Gc Switch Modules (NDPP11e3) Security Target*, Version 0.3, February 5, 2016.

[6] *Evaluation Technical Report for Hewlett Packard Enterprise Moonshot 180XGc, 45XGc, 45Gc Switch Modules*, Version 1.2, February 15, 2016

[7] *Assurance Activity Report for HPE Moonshot-180XGc, 45XGc, 45Gc Switch Modules*, Version 0.3, 02/15/2016