ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Galleon Embedded Computing XSR and G1 Hardware Encryption Layer

Maintenance Report Number: CCEVS-VR-VID11272-2024

Date of Activity: 22 July 2024

References:

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

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (FDEEEcPP20E/FDEAAcPP20E)

Impact Analysis Report for Galleon Embedded Computing XSR and G1 Hardware Encryption Layer, Revision 1.1, 07/18/2024

Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target, Version 1.6, June 27, 2024

Galleon Encryption Module v4 Release Notes, June 25, 2024

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in June 2024. The IAR is intended to satisfy the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target (ST) and the Impact Analysis Report (IAR). The ST was updated to reflect the new version of the TOE.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: *Galleon Embedded Computing XSR and G1 Hardware Encryption Layer Security Target*, Version 1.6, June 27, 2024	Version of product updated in Section 1.3. OpenSSL, OpenSSH, and net-snmp versions updated in Section 5.2.4.1
Design Documentation: See Security Target	No changes required
Guidance Documentation: **None**	No changes required
Lifecycle: None	No changes required
Testing: None	Galleon performed two levels of regression testing. See Regression Testing below.
Vulnerability Assessment: None	The public search was performed on 18 July 2024. No public vulnerabilities exist within the product. See analysis of results below.

Changes to the TOE:
Galleon Embedded Computing made updates to address CVEs and add performance fixes. The TOE product version was updated to 4.0.14, summarized below.

Major Changes

None.

Minor Changes

Galleon G1 Changes	
Change Description	**Security Analysis**
Updated OpenSSL to version 1.1.1w	This upgrade was done to address CVEs as required by NIAP. No algorithm implementations have changed. The upgrade does not impact SFRs; as such, re-evaluation is not required.
Updated OpenSSH to version 9.7p1	This upgrade was done to address CVEs as required by NIAP. The upgrade does not impact SFRs; as such, re-evaluation is not required.
Updated net-snmp to version 5.9.4	This upgrade was done to address CVEs as required by NIAP. The upgrade does not impact SFRs; as such, re-evaluation is not required.
Fix issue handling RDMs with unexpected serial formatting - At the factory Galleon programed the RDM serial number into the RDM EEPROM. This is used during authentication to look up the appropriate DEK in the key database. Galleon had some RDMs that were programmed incorrectly at the factory with a different format, and this caused the Encryption Module to stop reading serial numbers until power-cycled, even if the RDM was changed. This fix made the EM more robust to unexpected RDM EEPROM content	This is not a major security change because this is a performance fix. The device was not in an insecure state – it simply required a reboot which is not user-friendly. The fix does not impact SFRs; as such, re-evaluation is not required.
Fix rare keying error - After authentication, the DEKs are transferred from the processor to the Enova MX+ crypto chips over an I2C bus. Very rarely this transfer was showing an error. Galleon increased the delay from when they bring the MX+ chips out of reset until we transfer the DEKs by 500 ms to mitigate this issue	This is not a major security change because this is a performance fix. The device was not in an insecure state – it simply required a reboot which is not user-friendly. The fix does not impact SFRs; as such, re-evaluation is not required.
Fix SNMP not accessible from external network - During the evaluation SNMP was actually mis-configured and only listened on the local loopback interface. Hence it was not accessible over the network. No one noticed this, since the evaluated configuration is with Ethernet disconnected. The configuration was	This is not a major security change because in the evaluated configuration, SNMP is not available.

fixed so that SNMP was available on the network as documented and intended, although the Ethernet port must still be disconnected to match the evaluated configuration	

Regression Testing:
Galleon performs two levels of regression testing. Each encryption layer (in this case hardware) is tested independently during development. After successful single layer testing, the product is tested using “user stories" that cover expected functionality from the user's point of view and covers system integration issues.

Equivalency:

The security functionality of the current Galleon Embedded Computing XSR and G1 Hardware Encryption Layer update remains the same as the prior evaluated version. The models and processors are unchanged from the original evaluation version.

NIST CAVP Certificates:

The same cryptographic modules are used in the current Galleon Embedded Computing XSR and G1 Hardware Encryption Layer update. The CAVP certificate numbers referenced during the Galleon Embedded Computing XSR and G1 Hardware Encryption Layer evaluation have not changed.

Vulnerability Analysis

A search for known publicly disclosed vulnerabilities was performed against the National Vulnerability database and the Vulnerability Notes Database on July 18, 2024. The search terms used were:

- disk encryption
- drive encryption
- key destruction
- key sanitization
- Password caching
- Key caching
- Galleon
- G1
- XSR
- Intel Atom CPU C2758
- Intel Xeon CPU E3-1505L v6
- ARMv7 Processor rev 1
- Opal management software
- SED management software
- SNMP
- SATA

Of the results found for those search terms, none were identified as applicable to the changed TOE or were fixed by the patches applied as described in the change descriptions above. There are no publicly disclosed cybersecurity vulnerabilities applicable (in use) to the changed TOE. Therefore, no additional mitigation is required to the changed TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.