ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Klas Fastnet Series Switches KlasOS 5.3

Klas Fastnet Series Switches KlasOS 5.3

Maintenance Report Number: CCEVS-VR-VID11188-2023

Date of Activity: 26 July 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, September 12, 2016
- Impact Analysis Report for Klas Fastnet Series Switches KlasOS 5.3, Version 1.0, June 30, 2023
- Klas Fastnet Series Switches KlasOS 5.3 Security Target, Version 1.7, July 16, 2021
- Klas FastNet Series Switches KlasOS 5.3 Common Criteria Configuration Guide, Version 1.0, August 9, 2021
- collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 [NDcPP]

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR) for the Klas Fastnet Series Switches Voyager TDC 10G and Voyager TDC 12GG running KlasOS 5.3 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on June 30, 2023. 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 3.0. In accordance with those requirements, the IAR documents any 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 originally published Security Target (ST), the originally published Administrator's Guide, and an Impact Analysis Report (IAR) prepared by Gossamer Security Solutions.

Documentation updated:
No changes to the TOE documentation were reported by the developer.

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Klas Fastnet Series Switches KlasOS 5.3 Security Target, Version 1.7, July 16, 2021	**Maintained Security Target:** Klas Fastnet Series Switches KlasOS 5.3 Security Target, Version 1.7, July 16, 2021 Changes in the maintained ST are: • No changes reported.
Common Criteria Compliance Guide: Klas Fastnet Series Switches KlasOS 5.3 Common Criteria Configuration Guide, Version 1.0, August 09, 2021	**Maintained Common Criteria Compliance Guide:** Klas Fastnet Series Switches KlasOS 5.3 Common Criteria Configuration Guide, Version 1.0, August 09, 2021 Changes in the maintained Guidance are: • No changes reported.

Changes to the TOE:
No changes to the TOE or the TOE development environment were reported by the developer.

Regression Testing:
No regression testing is required.

NIST CAVP Certificates:
CAVP certificates are unchanged, and no additional review or testing is required.

Vulnerability Analysis:
A new search was performed for vulnerabilities from the time of the original evaluation (05 August 2021). This search was performed on 30 June 2023. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected.

The search was conducted against:

- NIST National Vulnerabilities Database (http://web.nvd.nist.gov)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The following search terms were used:

- "Klas", "KlasOS", and "KLAS-VOY-TDC-R2.0" as variations of the TOE name.
- Processors:
  - Marvell Prestera 98DX8212
- Software:
  - OpenSSH 7.7p1
  - OpenSSL 1.0.1u
  - Linux 3.10.70
  - Linux-PAM 1.3.1
  - GNU C 2.13
  - Rsyslogd 8.34.0

Conclusion:

The overall impact is minor. This is based on the rationale that no changes or updates were made to the TOE, the TOE developer environment, or its documentation. As such, the security posture and policies of the TOE are unchanged from their original evaluation. Additionally, no outstanding vulnerabilities associated with the version of the TOE or underlying TSF presented for Assurance Maintenance have been disclosed or reported by the vendor.

The CCEVS agrees that the original assurance is maintained for the product.