ASSURANCE CONTINUITY MAINTENANCE REPORT FOR 3eTI CyberFence 3e-636 Series Network Security Devices

---

Maintenance Update for: CyberFence 3e-636 Series Network Security Devices

Maintenance Report Number: CCEVS-VR-VID10820-2018

Date of Activity: 18 June 2018

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- 3e Technologies International CyberFence 3e-636 Series Network Security Device Impact Analysis Report, Revision A, May 21, 2018 Version 1.0;
- 3eTI-636 Vulnerability Analysis Report, May 24, 2018;
- collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015

Documentation reported as being updated:

- None

Assurance Continuity Maintenance Report:

3e Technologies International, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 1 June 2018. 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 2.0. In accordance with those requirements, the IAR describes any changes made to the certified TOE, any evidence updated because of the changes, and the security impact of any changes.

Introduction:

Due to the potential impact of the Spectre and Meltdown vulnerabilities, the vendor performed an assessment on the product to ensure that the product was resistant to those vulnerabilities using the tools and analysis methods available as of the time of this report.

The IAR stated that no changes were made to the TOE with respect to the Spectre and Meltdown vulnerabilities and that a public search for vulnerabilities discovered since the original posting was negative or the findings not applicable to the product.

Summary Description:

The vendor asserts that changes to the TOE were not required to address those vulnerabilities because:

- testing using a Spectre detection tool (which was recompiled by 3eTI for the 32 bit processor) produced negative results. The detection tool source code originated with example code described in: "*Spectre Attacks: Exploiting Speculative Execution*" (https://spectreattack.com/spectre.pdf). That code, and subsequent modifications, were based upon sample code available at: https://gist.github.com/miniupnp/9b701e87f14ad3e0a455cfb54ba99fed.
- the TOE Freescale MPC8378 CPU e300 core, which is based upon PPC 603 32-bit core architecture, is not vulnerable to Meltdown attacks as detailed at the official Meltdown CVE information pages: https://nvd.nist.gov/vuln/detail/CVE-2017-5754/ and https://nvd.nist.gov/vuln/detail/CVE-2017-5754/cpes. In particular:
    - Meltdown is limited to certain Intel-only x86 products which perform out-of-order execution. Non-Intel x86 implementations (i.e. AMD) are not inherently affected, and the TOE's FreeScale CPU core is not on listed as vulnerable to Meltdown on the CVE page.
- the vendor claims that no additional relevant vulnerabilities were discovered during an updated search of the following sites:
    - National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
    - 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),
    - Exploit / Vulnerability Search Engine (http://www.exploitsearch.net),
    - SecurITeam Exploit Search (http://www.securiteam.com),
    - Offensive Security Exploit Database (https://www.exploit-db.com/)
    - Tenable Network Security (http://nessus.org/plugins/index.php?view=search),

Therefore, no security relevant changes were made to the TOE:

- no changes to hardware, software or firmware
- no model version identification changes,
- no additional platforms are claimed as part of this maintenance.

The evaluation evidence consists of the Impact Analysis Report (IAR) and supporting vulnerability analysis update, dated May 24, 2018.

The original evaluation was performed against the collaborative Protection Profile for Network Devices Version 1.0 and the ST referenced validated CAVP certificates. No changes were made to the processor and therefore no modifications were required to any of the valid NIST certificates.

Changes to TOE:
None

Affected Developer Evidence:
None

Regression Testing:
None performed, as no changes were made to the TOE.

Vulnerability Analysis:
An updated vulnerability analysis was conducted and no outstanding vulnerabilities were found related to the device; and through testing and additional analysis, the TOE was found to not be vulnerable to Meltdown and Spectre.

Conclusion:
CCEVS reviewed the vendor provided description of the analysis and testing for the Spectre vulnerability upon the devices, and found there to be no impact upon security related functionality. In addition, the TOE vendor reported having conducted a vulnerability search update that located no new applicable vulnerabilities requiring mitigation. All the security functions claimed in the ST remain enforced by the 3eTI CyberFence 3e-636 Series Network Security Devices. Therefore, CCEVS agrees that the original assurance is maintained for the product.