National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

CCEVS Policy Letter #17

12 January 2010

SUBJECT: Effects of Vulnerabilities in Evaluated Products

PURPOSE: Prevent products with known vulnerabilities from receiving a CCEVS Certificate. This written policy codifies the common practices currently implemented by CCEVS.

POLICY: All vulnerabilities within the TOE boundary discovered at any time before or during the course of the evaluation *must* be corrected before CCEVS will issue the Common Criteria (CC) certificate. CCEVS will not accept the re-scoping of the TOE boundary to exclude the vulnerability from the TOE.

Any vulnerability within the product yet outside the TOE boundary *should* be corrected. While the vendor will be encouraged to fix the vulnerability, issuance of the CC certificate will not depend on the vulnerability being corrected. In cases where the vulnerability is not corrected, CCEVS will post an advisory on the Validated Products List (VPL) and will explicitly note the presence of the vulnerability in the published Validation Report (VR).

RATIONALE: A CC certificate carries with it an expectation of the quality of the evaluated product. As such, our customers presume the evaluated product was free from known vulnerabilities at the time the certificate was issued. Although it is not unusual for vulnerabilities to be discovered after the certificate has been issued, it is inexcusable for CCEVS to issue a certificate for a product known to contain vulnerabilities.

It should be noted this policy is not an interpretation of a CC requirement rather it is specific to those products evaluated within the US CCEVS.

EFFECTIVE DATE: This written policy takes effect immediately.
.

Original Signed By

CAROL SAULSBURY HOUCK
Director