

CAE-71: FISMA Monitored Unsecurable Custom Application



This page has been made public for vendors

Abstract

The VA application has been (or if the application is in development, is intended when in production to be) deployed to a **FISMA-reportable system**, but is not scannable using VA-licensed Static Application Security Testing (SAST) tools according to **VA Secure Code Review SOP**.

Unsecurable applications require compensating security controls elsewhere in the IT environment, outside of the source code. Unsecurable applications are subject to alternate compensating technical testing that should be performed according to applicable approval procedures and conditions.

Explanation

All VA applications should ultimately belong to a FISMA-reportable system. The term "monitored" refers to applications that have been deployed to a FISMA-reportable system and as such their operation is being monitored by VA accordingly as components of the system.

VA applications are written in different programming languages, in different development environments, and so on. The term "unsecurable" refers to applications whose source code cannot be scanned using the VA-licensed HP Fortify Static Code Analyzer (SCA) tool, such as those written in MUMPS and Delphi.

Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP, and enforced as part of the ATO issuance process.

References

1. **VA Secure Code Review SOP**
2. "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.
3. "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.
4. HP Fortify System Requirements, current software release.