

# Fortify Rulepack Version 2016.3.0 Released

This VA Software Assurance Notification is an announcement about the release of updated HPE Fortify Static Code Analyzer (SCA) rulepacks. 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.

Fortify scans that do not use this new release of the Fortify software will result in scan issues for secure code review validation submission packages accepted\* after **October 11, 2016**. Accepted is defined as all required secure code review validation prerequisites have been met. For information about requesting secure code review validations, please see [here](#).

The most recent version of Fortify, and the complete, most recent set of the Fortify rulepacks must be used when scanning code. As of this release, the Fortify Secure Coding Rulepacks detect 709 unique categories of vulnerabilities across 23 programming languages and span over 840,000 individual APIs. Release notes can be viewed [here](#). The release includes the following:

- iOS Watchkit
  - Support for WatchKit, WatchConnectivity and ClockKit frameworks for Objective-C and Swift rulepacks.
  - Category coverage for Privacy Violation, System Information Leak, and System Information Leak: External.
  
- LDAP Entry Poisoning
  - New vulnerability category coverage for detecting the potential for attackers in control of an LDAP entry to compromise vulnerable applications by performing a search on the entry.
  
- Extended support for improperly configured encryption keys
  - Improper use cryptographic APIs, related to key management, can reduce the security of applications.
  - Additional rule coverage has been added to ABAP, ActionScript, CFML, JavaScript, SQL, and VB6.
  
- ASP.NET insecure settings
  - Access Control: Form Authentication Bypass and ASP.NET Misconfiguration: Missing HMAC Signature have been introduced to detect insecure settings.
  - Improved rule coverage to detect insecure settings are available for Denial of Service, Dynamic Code Evaluation: Unsafe Deserialization, and Open Redirect.
  
- DISA STIG 4.1
  - Supported correlation between HPE Security Fortify Taxonomy categories and the STIG IDs from the latest Defense Information Systems Agency Application Security and Development STIG, version 4.1.