Features

- Plug-n-Play firmware security testing for x86/x64 architectures
- Includes latest security tests and CHIPSEC for comprehensive vulnerability protection
- Provides clear, concise and immediate test reports
- Powerful tool in the fight against regression of security defects
- Perform all security test in under 10 minutes
- Easily update to include the latest security tests

ami | FirST™

Firmware Security Testing

The Best Security Testing – with AMI FirST
AMI Firmware Security Testing (FirST) is a suite of test tools for verification of production UEFI firmware security for x86/x64 architectures. AMI FirST tests are kept current with the latest developments in firmware security threats for comprehensive testing and prevention of security defect regression and vulnerability.

Log information and test results from AMI FirST are provided in a simple, concise format. Each test is clearly delineated with pass, fail or not applicable status. Every failed test directs the user to the corresponding AMI Security Advisory for remediation of the issue and any additional required action.

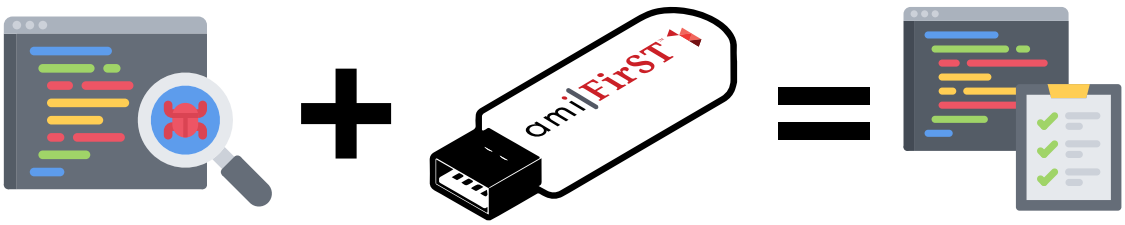
AMI FirST Test Tools in Detail
AMI FirST Test Tools are an important addition to any OEM development team or quality assurance (QA) lab, to confirm that any potential firmware security issues are properly mitigated. Most test tools are black box UEFI test applications that run via UEFI shell. The black box tests are designed to be as simple to run as possible so that an engineer is not required.

The user can select which AMI FirST Test Tools to run simply by modifying a configuration file in the UEFI shell. Once the selected list of tests is complete, a clear and concise log file with all test information is delivered to the user, with all pass, fail and not applicable results included.

In the case of a failed test, the test report log will direct the user to the corresponding security advisory to assist in remediation of the issue. In some limited cases, the user may be required to take additional manual steps using third-party tools that might require the installation of an operating system (OS) for completion.

The addition of third-party tests in AMI FirST improves product security and ensures that virtually no issues are missed in regression testing. This allows the development team to focus on the latest vulnerabilities for a given product, and the QA team to ensure that all potential security issues are resolved.

Note that some security issues do not have an equivalent black box test, but a corresponding test may be available that requires a check of the source to ensure that the issue is properly patched.



*USB Stick not included. AMI FirST is provided as a download.

ami™
power • manage • secure

Simple Deployment, Update and Test Result Delivery Process

The deployment process for AMI FirST is simple and quick. Using the UEFI shell, the AMI FirST suite of tools boots easily from USB or a similar mass storage device and takes less than 10 minutes to download and deploy.

Customers also have the option to submit their platforms to AMI and have AMI engineers perform the tests for them. AMI is also working on a cloud-based solution that will be available in the near future.

AMI distributes all applicable tests written and developed by AMI to the customer. There are additional collateral materials that integrate state-of-the-art tests. AMI does provide recommended third-party proprietary versions of test tools, with the results merged in with AMI's result information.

Once an update package become available, customers should download the updated tests and extract them to a USB drive or similar mass storage device.

Example of AMI FirST in Action

5555 Oakbrook Parkway
Building 200
Norcross, GA 30093 USA
Tel: 770.246.8600
Sales/Toll Free : 800.828.9264
ami.com