Security Report - Kernel

Updated: May 14, 2020

Revision 0.50

Revision History

Revision	Date	Description
0.51	07-Apr-21	Add gFvbAccessThroughSmiGuid and gEfiSmmVariableProtocolGuid related SMI Reprots
0.50	14-May-20	Initial Revision Add Software SMI Report - FBTSGetPlatformInfo (AL=0xEF, AH=0x11) Add Software SMI Report - FBTSApHookPoint (AL=0xEF, AH=0x1F)

Overview

- Build Settings
- General Review Items
- High-Risk Technology Area Review
  - Software SMIs
  - UEFI Variables
  - Flash Updates
  - S3
  - Network
  - Crisis Recovery
  - External Hardware inputs

Build Settings

- List the versions of all tools used in QA results
  - Microsoft Visual Studio (C compiler, linker, nmake)
    - DEVTLS_VC14 (VS2015)
  - ASL compiler
    - Intel ASL+ Optimizing Compiler version 20160422-32
  - Python
    - Python 2.7.6
  - FIT tool
    - Intel Flash Image Tool version 12.0.40.1434

General Review Items

- C#1 Trust Boundary Crossing
- C#2 Compiler Security Settings
- C#3 Hardware Protections
- C#4 Approved Cryptography
- C#5 Reduced Attack Surface
- C#6 Secure By Default
- C#7 Defense-in-Depth
- C#8 Examine Past Vulnerabilities
- C#9 Deprecate Outdated Functionality
- C#10 Review Sample Source Code
- C#11 Canonicalization
- C#12 Up To Date On Security Issues
- C#13 Keep The Team Educated
- C#14 Do Not Use Banned Functions
- C#15 Check Overridden Files For Updates

Software SMI Review Items

- SMI#1 Call Code Outside SMRAM
- SMI#2 Access Data Outside SMRAM
- SMI#3 MMIO Access via Base-Address Registers (BARs)
- SMI#4 Communication Buffer Allocation
- SMI#5 Communication Input Buffers
- SMI#6 Communication Output Buffers
- SMI#7 Communication Input Buffer Overlap
- SMI#8 Communication Input/Output Buffer Overlap
- SMI#9 Communication Input/Output Buffer Null-Terminated Strings
- SMI#10 Communication Input/Output Buffer Variable-Length Data Structures
- SMI#11 Multi-Stage Software SMI Operations
- SMI#12 Security Error Handling
- SMI#13 Security Levels
- SMI#14 Memory Allocation
- SMI#15 Remove Unused SMI Handlers
- SMI#16 Move To DXE or Runtime
- SMI#17 Reserved MMIO
- SMI#18 Copy Parameters Before Use
- SMI#19 Close Unnecessary Service
- SMI#20 SMRAM Lock
- SMI#21 Communication Input Buffer Error Checking

Software SMI Items – Report (1)

- FBTSGetPlatformInfo (AL=0xEF, AH=0x11)
- FBTSApHookPoint (AL=0xEF, AH=0x1F)
- ReadFdThroughSmi (gFvbAccessThroughSmiGuid, 0x00)
- WriteFdThroughSmi (gFvbAccessThroughSmiGuid, 0x01)
- EraseFdThroughSmi (gFvbAccessThroughSmiGuid, 0x02)
- SmmAddFileHashImage (gEfiSmmVariableProtocolGuid, 0x01)
- SmmUpdateSecureBootEnforce (gEfiSmmVariableProtocolGuid, 0x02)
- SmmClearAllSecureSettings (gEfiSmmVariableProtocolGuid, 0x03)
- SmmRestoreFactoryDefault (gEfiSmmVariableProtocolGuid, 0x04)
- SmmUpdatePkVariable (gEfiSmmVariableProtocolGuid, 0x05)
- SmmUpdateKekVariable (gEfiSmmVariableProtocolGuid, 0x06)
- SmmUpdateDbVariable (gEfiSmmVariableProtocolGuid, 0x07)

Software SMI Items – Report (2)

- SmmUpdateDbxVariable (gEfiSmmVariableProtocolGuid, 0x08)
- SmmUpdateDbtVariable(gEfiSmmVariableProtocolGuid, 0x0B)
- SmmUpdateDbrVariable(gEfiSmmVariableProtocolGuid, 0x0C)
- SmmClearDeployedMode(gEfiSmmVariableProtocolGuid, 0x09)
- SmmSelectSecureBootMode(gEfiSmmVariableProtocolGuid, 0x0A)
- SmmSetSensitiveVariable(gEfiSmmVariableProtocolGuid, 0x21)
- SmmCreateVariableLockList(gEfiSmmVariableProtocolGuid, 0xFA)
- SmmLegacyBootEvent(gEfiSmmVariableProtocolGuid, 0xFB)
- SmmInternalSetVariable(gEfiSmmVariableProtocolGuid, 0xFC)
- SmmDisableVariableCache(gEfiSmmVariableProtocolGuid, 0xFE)
- SmmDisableSecureBootSmi(gEfiSmmVariableProtocolGuid, 0xFF)
- SmmUpdateVariablePropertySmi(gEfiSmmVariableProtocolGuid, 0xF8)

Exceptions: Software SMI (AL=0xEF, AH=0x11) FBTSGetPlatformInfo

- Exception to Rule SMI#08
  - Justification: The communication input and output buffers are overlapped by design. The handler validates input buffer is entirely inside the communication buffer and have sufficient space for output data.
- Exception to Rule SMI#15
  - Justification: This handler must be on by default. It may be removed by disabling IHISI or by using the PCD PcdH2OIhisiFbtsSupport.
- Exception to Rule SMI#16
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#20
  - Justification: This depends on other code to close and lock access to SMRAM.

Exceptions: Software SMI (AL=0xEF, AH=0x1F) FBTSApHookPoint

- Exception to Rule SMI#15
  - Justification: This handler must be on by default. It may be removed by disabling IHISI or by using the PCD PcdH2OIhisiFbtsSupport.
- Exception to Rule SMI#16
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.
- Exception to Rule SMI#20
  - Justification: This depends on other code to close and lock access to SMRAM.

Exceptions: SMM communication ReadFdThroughSmi

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation..
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication WriteFdThroughSmi

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation..
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication EraseFdThroughSmi

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation..
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication SmmAddFileHashImage

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation..
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateSecureBootEnforce

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation..
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmClearAllSecureSettings

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmRestoreFactoryDefault

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdatePkVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateKekVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateDbVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateDbxVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateDbtVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmUpdateDbrVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmClearDeployedMode

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at Administer Secure Boot Menu and cannot be closed at end-of-DXE. Instead, close at Ready-To-Boot.

Exceptions: SMM communication SmmSetSensitiveVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication SmmCreateVariableLockList

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.

Exceptions: SMM communication SmmInternalSetVariable

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication SmmDisableVariableCache

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

Exceptions: SMM communication SmmDisableSecureBootSmi

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.

Exceptions: SMM communication SmmUpdateVariablePropertySmi

- Exception to Rule SMI#11
  - Justification: The SMM code is not a part of a multi-stage software SMI operation.
- Exception to Rule SMI#18
  - Justification: Not necessary based on x86 threat model. It relies on IOMMU Settings to protect against DMA attacks. It relies on all x86 CPU threads being in SMM before this SMM code is called. It does not protect against auxiliary processor attacks.
- Exception to Rule SMI#19
  - Justification: This handler is used at runtime and cannot be closed at end-of-DXE.

UEFI Variable Review Items

- UV#1 Correct Variable Attributes
- UV#2 Controls Security Policy
- UV#3 Contains Passwords or Secrets
- UV#4 Same Security Every Boot Path
- UV#5 Variable Size Changes
- UV#6 Variable Deleted
- UV#7 Invalid Variable Values
- UV#8 Deprecated library functions.
- UV#9 Variable Has Default Value
- UV#10 Variable Error Handling
- UV#11 Variable Store Corruption
- UV#12 Variable Store Full
- UV#13 Authenticate Variables

Flash Update Review Items

- FU#1 Flash Image Version
- FU#2 Flash Image Integrity
- FU#3 System Flash Updates
- FU#4 Device Flash Updates
- FU#5 Device, Partition and File Error Handling
- FU#6 Partial Flash Update
- FU#7 Flash Locking

S3 Review Items

- S3#0 Flash Update and Software SMI
- S3#1 S3 Data Corruption
- S3#2 S3 Protections

Network Review Items

- NET#1 Network Responses
- NET#2 Network Packet
- NET#3 Network Response Packets
- NET#4 Network or Wi-Fi Passwords
- NET#5 Network or Wi-Fi Passwords Hardcoded
- NET#6 Network or Wi-Fit Passwords Cleared
- NET#7 Network or Wi-Fit Passwords Comparison
- NET#8 Network or Wi-Fi Password Criteria
- NET#9 Network or Wi-Fi Password Hashing
- NET#10 Network Public Certificates
- NET#11 Network Private Certificates

Crisis Recovery Items

- CR#0 Flash Update
- CR#1 Hardware Protections

External Hardware Input Items

- HI#1 Hardware Input Error Handling
- HI#2 Hardware Input Checking On All Paths
- HI#3 Usage Of ASSERT
- HI#4 USB Descriptors
- HI#5 Bluetooth Advertisement Messages
- HI#6 Storage DMA
- HI#7 Storage Security
- HI#8 Storage Security Password
- HI#9 PCIe Option ROMs
- HI#10 DIMM SPD Error Handling
- HI#11 Storage Identify Drive Information
- HI#12 MMIO BAR Setup