Phoenix Security Training

WHO SHOULD ATTEND

This training is intended for Firmware Engineers and Firmware Managers who want to learn about UEFI Security Vulnerabilities, Features, and Best Practices to build more Secure UEFI Firmware by reducing the Attack Surface and utilizing Vulnerability Mitigation Strategies.

OVERVIEW

- Three-day class
  - Structured classwork
  - Lab work
- Attendees will learn about
  - UEFI Attack Surface and Attack Vectors
  - UEFI Firmware Changing Landscape
  - Key Industry Insights
  - UEFI Hardware and Software Security Features
  - UEFI Exploits and Mitigation Strategies
  - Best Practices for Implementing Secure UEFI Firmware

PARTIAL SYLLABUS

- UEFI Threat Modeling
- Historical UEFI Vulnerabilities
- Phoenix UEFI Security Features
- Intel UEFI Security Features
- Common UEFI Secure Coding Issues
- UEFI Best Practices

DETAILS

- Location of the training will be arranged with the attendees, either at a Phoenix facility or at the attendees' facility
- Dates of the training will be arranged with the attendees
- Quotation for the cost of the training can be obtained from your local Phoenix salesperson
- Requires a minimum number of attendees, as determined by Phoenix
- Requires execution of a contract by the parties, as provided by Phoenix

BRIEF AGENDA

Day 1

- UEFI Threat Modeling
- UEFI Threats and Vulnerabilities
- Attack Mitigation
- Security Vulnerability Disclosures
- UEFI Variables
- Cryptographic Libraries
- Runtime Environment
- SMM Hardware and Software Protections
- SMM Threat Model

Day 2

- SecureBIOS, SecureFlash, and SecureBoot
- Secure Capsule Update Protection
- Variable Service Security Features (EDKII)
- Memory Overwrite Request (MOR) Protection
- Windows UEFI Firmware Update
- Securely Processing Sensitive Information
- Correct Usage of Cryptographic Algorithms
- Buffer Overflows
- SMM Incursion Vulnerabilities

Day 3

- Avoid Adding New Flaws
- Find Existing Flaws
- Employ Mitigations
- Security Vulnerability Reports and Analysis
- Exposure and Impact
- Security Process Strategy
- Security Incident Response Plan
- Product Security Maintenance and Tracking
- Releasing and Deploying Patches

Phoenix Technologies Ltd.

Americas
150 South Los Robles Ave, Suite 500
Pasadena, California 91101
Toll Free 1-800-677-7305
Tel +1-408-570-1000
Fax +1-408-570-1001
E-mail sales@phoenix.com

Taiwan
7F., No. 88, Ruihu St.,
Neihu District,
Taipei City 114,
Taiwan, R.O.C.
Tel +886-2-7745-5600
Fax +886-2-7745-5699

Korea
2F, Cheongwon Bd.,
33 Teheran-ro 8-gil,
Gangnam-gu
Seoul 06239, Korea
Tel +82-2-3014-4700
Fax +82-2-3461-8676

Japan
Gotanda NN Building 8th Floor
2-12-19, Nishi-Gotanda,
Shinagawa-ku
Tokyo 141-0031 Japan
Tel +81-3-5435-6700
Fax +81-3-5435-6701

www.phoenix.com