The UEFI Security Response Team (USRT)

Dick Wilkins, Ph.D.
Principal Technology Liaison
Phoenix Technology Ltd.

presented by

UEFI Plugfest – October 2014

Agenda

What is the USRT?

How did it come about?

Who are the members?

What does the USRT do?

How are inputs processed?

What is left to do?

Call to Action

Thanks to Phoenix Technologies!

This presentation is made on behalf of the UEFI Forum and not my company.

But, I want to thank Phoenix Technologies for providing the time for me to chair the USRT subcommittee and for supporting my travel to make this presentation possible.

What is the USRT?

- The UEFI Security Response Team is a subcommittee of the forum’s board of directors
- It is **NOT** a traditional “working group” and does not follow the membership and voting rules of those teams
- It’s primary purposes are to:
  - Provide a point-of-contact for security researchers to report issues and vulnerabilities to the membership of UEFI
  - It will work with UEFI members to enhance and coordinate responses to actual and perceived vulnerabilities

How did it come about?

- As use of UEFI firmware becomes more widespread, it has become at target of hackers (“white hat” and “black hat”)
- The “white hat” folks want to tell us about problems they have found before going public
- Most of those folks do not understand the complex supply chain of firmware into consumer products
- They are technically savvy but lack the right contacts with ODMs, IBVs and some OEMs
- The USRT is a response to this demonstrated need
- It was created at the May 2014 Plugfest

Who are the members?

- As a subcommittee of the UEFI board, all **promoter** member companies are welcome to participate
- Other companies may be invited to join
- Current participating companies:
  - AMD
  - American Megatrends
  - Dell
  - Hewlett-Packard
  - Insyde
  - Intel
  - Lenovo/IBM
  - Microsoft
  - Phoenix Technologies
  - RedHat

What do we do?

- We have created a web page on the UEFI site soliciting inputs from the security research community
- We have reached out to these researchers, CERT/CC and others to let folks know we are operational
- We are joining “FIRST” to increase our visibility and ensure we are using “best practices”
- We have started processing vulnerability reports

How are inputs processed?

- Inputs are sent to security@uefi.org and are received by a rotating list of designated USRT members
- A MANTIS ticket is created to track the incident and they are acknowledged to the reporter
- A summary of the issue is sent to UEFI contributor members who have opted-in to receive this information
- The USRT will follow up with effected member companies to ensure any vulnerabilities are being handled
- Every effort is made by the USRT to protect sensitive information to minimize the possibility of zero-day attacks

What is left to do?

- We need to develop a better process for following up on reported vulnerabilities
- We need an outreach education program to educate security researchers and others about the constraints of the industry today
- We need to create and set expectations of responsiveness to reports by UEFI member companies
- We need to explore ways to coordinate the rollout of fixes by independent members to protect the public from zero-day attacks
- The industry, with UEFI and USRT participating, needs to develop better approaches to allow and encourage the speed and widespread adoption of firmware updates

Call to Action

- Contributor members should join the opt-in list if they have not done so (email admin@uefi.org)
- All UEFI member companies need to develop policies and procedures for efficiently dealing with reported security vulnerabilities
- Everyone needs to participate in the discussion on how to rapidly develop, deliver, coordinate and encourage the uptake of security fixes

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

The UEFI Forum and

phoenix® technologies