UEFI Security Response Team (USRT)

Fall 2017 UEFI Plugfest

October 30 – November 3, 2017

Presented by Dick Wilkins, PhD (USRT Chair / Phoenix Technologies)

Topics

- What is the USRT?
- How did it come about?
- Who are the members?
- What does the USRT do?
- How are inputs processed?
- Call to Action

What is the USRT?

- The UEFI Security Response Team is a subcommittee of the forum’s board of directors
- It is **NOT** a traditional specification “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 and others, 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?

- Black Hats vs. White Hats
  - As use of UEFI firmware has become ubiquitous, it is the target of hackers (“white hat” and “black hat”)
  - The “white hat” folks want to tell us about problems they have found before going public (they want credit for their work)
  - Most of these folks do not understand the complex supply chain of firmware into consumer products
  - Vulnerability reporters are technically savvy but lack the right contacts with ODMs, IFVs and some OEMs
  - The black hatters are, of course, those who are evil doers
- Why the USRT?
  - The USRT is a response to this demonstrated need
  - It was created during a board meeting 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
  - Apple
  - ARM Limited
  - Dell
  - HP, Inc.
  - Insyde Software
  - Intel
  - Lenovo
  - Microsoft
  - Phoenix Technologies
  - Red Hat

What do we do?

- We have created a web presence on the UEFI site soliciting inputs from the security research community
- We provide a PGP key for their use in securely reporting potential vulnerabilities
- We have reached out to these researchers, CERT/CC and others to let folks know we are operational
- We have joined the Forum of Incident Response and Security Teams (FIRST) to increase our visibility and ensure we are using “best practices”
- We have developed a relationship with Tianocore, the open-source UEFI reference implementation group

Incidents to date

- We have handled roughly 40 “incidents” in the USRT’s three years in existence
- A handful were just informative
- A couple were determined “bogus”
- The rest were real bugs that needed to be fixed

How are inputs processed?

- Inputs may be sent to security@uefi.org or by other paths and are received by a rotating list of designated USRT members
- A Mantis ticket is created to track the incident and the issue is acknowledged to the reporter
- The USRT team reviews the content of the report and decides on appropriate further processing
- The Mantis ticket number may be sent to UEFI contributor members who have opted-in to receive this information
  - This notification is done for issues that are deemed critical or important and those that may be of general interest to the UEFI community
- Every effort is made by the USRT to protect sensitive information to minimize the possibility of zero-day attacks

Other USRT responsibilities

- The USRT will attempt to coordinate responsible disclosure of vulnerability details between UEFI members and reporters
- The USRT will **NOT** attempt to coordinate release dates of fixes between members

Tianocore bug fixes

- The open-source reference platform provides the basis of many product implementations
- Vulnerabilities found in this code may affect large numbers of products from many manufacturers
- The “bad guys” monitor code check ins for vulnerabilities they can exploit in products already shipping
- USRT’s goal is to minimize these opportunities
- We have negotiated the following policies…

Tianocore embargo policies

- When a vulnerability is found in newly released open-source code that is unlikely to be in shipping products
  - Release the update ASAP so as to get the fix into as many hands as possible
- When a vulnerability is found in code in the public domain that is likely in shipping products
  - The USRT will track and report the vulnerability
  - A fix will be developed as quickly as possible and delivered to the UEFI contributor community
  - The fix will be embargoed from the public code base for a period of six (6) months to allow time for it to be adopted and rolled out to shipping products

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
- Consider reporting known vulnerabilities via the CVE system, https://cve.mitre.org/

Thanks for attending the Fall 2017 Plugfest

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

presented by