Meltdown and Spectre vulnerabilities - Lessons learnt

Linda Cornwall

EGI CSIRT F2F January 2018 - CERN

Timeline for basic SVG actions

- 2018-01-03 07:59 Received info from Raul Lopes
- 2018-01-03 15:54 ‘Heads up’ sent
- 2018-01-04 15:03 ‘Advisory’ sent with 7 day deadline
- 2018-01-09 15:34 WLCG Advisory
- 2018-01-10 Created wiki for Meltdown and Spectre
- 2018-01-11 14:31 Advisory update sent
  - pointing to wiki info
  - Removing deadline
- 2018-01-23 08.01 Advisory Update 2 sent
  - Re-setting deadline for kernel patches for Meltdown(Variant 3) and Spectre(Variant 1)

(times GMT)

Wiki page for Meltdown/Spectre

- Created wiki, with information rather than lots of info in an advisory
  - Mainly links to public information
  - Various SVG members keep adding updates
- Situation changing
  - Intel pulled patches
  - Various product teams changed their advice
  - Situation still not fully resolved

Decided Update advisory if/when

- We are telling people to do something different from last time
- We want to tell people something which we want to be AMBER, i.e. we can't put on the wiki.
- We wanted to re-set a deadline

CSIRT re-set deadline

- CSIRT re-set deadline, after testing they could monitor kernel versions for Meltdown(3) and Spectre(1) mitigation
  - It may have been possible to keep deadline in the first place, but only for these kernel mitigations
- Split advice on what to do concerning
  - Kernel to mitigate Meltdown(3) and Spectre(1) – re-setting deadline
  - Spectre(2) and microcode – stating sites should follow their software and hardware vendors

What went well?

- Timely initial ‘Heads up’ and ‘Advisory’
- Lots of interested people
- Wiki for providing info

What went less well?

- Time between removing deadline and re-setting
  - One SVG member thinks this is too long (12 days)
  - Some hoped situation would get clearer, be more fully resolved
  - Kernel patches were available, even if microcode patches were not
  - CSIRT re-set after testing kernel patch monitoring
- Masses of e-mails on the subject
  - Discussions
  - Results of performance tests
  - Difficult to disseminate what is useful

Future

- The AMBER Advisory plus wiki for public info is a possible way to do things in future in some situations
  - Software in widespread use
  - Vulnerability is public
  - Lots of public information
  - Changing public information
  - Don’t want to keep sending advisories

What to discuss?

- Do you agree the wiki info way is a good model for other public vulnerabilities?
  - I.e. separate info that is public on wiki
  - Advisory still amber
- Maybe we should have had an ad-hoc meeting to discuss these vulnerabilities?
- Would it make sense to have a private wiki?
  - Maybe that site admins can access?
  - This won't be automatic, SSO group which we and CSIRT can add to.

What to discuss?

- Can we collaborate better with others?
  - WLCG, EUDAT…..
- What else?

Thank you for your attention.

Questions?

www.egi.eu