Systems-Facing call, 2026-06-18 @ 1p ET/ 12p CT/ 11a MT/ 10a PT

Topic: **Myth vs Mythos: The Reality of CVEs and Research Computing**

The number of CVEs affecting HPC and research computing systems has recently spiked, and fears about the risks that AI poses to internet security have risen enough to garner media coverage. These two factors have resulted in HPC and research computing practitioners dealing with both significant patching activity and increased expectations to implement mitigations quickly. Does the current landscape warrant a change in how cybersecurity is approached, is a tightening of existing practices sufficient, or is there really a rise in vulnerabilities? This session will explore how institutions, labs, and research centers are dealing with the situation and offer perspectives on the current research cybersecurity landscape.

Moderator:
- Matthew Ellis, Manager, Cybersecurity Incident Management, University of British Columbia

Panelists:
- Ben Nickell, HPC Systems Administrator, Idaho National Laboratory;
- Andrew Bruno, Assistant Director, Software Engineering & DevOps, Center for Computational Research, University at Buffalo;
- Matt West, HPC Systems Administrator, UNC Charlotte;
- Maxime Boissonneault, Team lead for Research Support National Team (Digital Research Alliance of Canada), Directeur des services à la recherche et à l'enseignement (Calcul Québec), Spécialiste en HPC à l'Université Laval

Link To Video Recording: https://www.youtube.com/watch?v=0LRaBEVYurY

Zoom Meeting Room:

https://utah.zoom.us/my/carcc?pwd=TjFuR3VVM2d5eE5zWnEvWWxDTFBCUT09

Meeting ID: 824 051 8198
Password: 31415926

One tap mobile
+13462487799,,8240518198#,,#,31415926# US (Houston)
+16699006833,,8240518198#,,#,31415926# US (San Jose)

Dial by your location
+1 346 248 7799 US (Houston)
+1 669 900 6833 US (San Jose)

NOTE: **This meeting will be recorded via Zoom.**

Link To Slides:
TBA

CaRCC YouTube Channel: https://www.youtube.com/carcc

CaRCC YouTube Channel Systems-Facing Playlist:
https://www.youtube.com/playlist?list=PLV-SC0CHLTwehApeMg_fJ5VbYndETh3yT

CaRCC YouTube Channel Data-Facing Playlist:
https://www.youtube.com/playlist?list=PLV-SC0CHLTwdrPXN8zdres6aovVAoEJIq

CaRCC Code of Conduct: https://carcc.org/about/carcc-code-of-conduct/

Join the CaRCC Slack Workspace:
https://join.slack.com/t/carcc/shared_invite/zt-9lhv4cfm-wy7RpbNI7V9qLJcvtzq8hA

Sign-In (Name / Affiliation / Email): (Max on call: 97)

1. Andrew Ferris /UBC Centre for Heart-Lung Innovation/ andrew.ferris@hli.ubc.ca
2. Nathan Wells / Kansas State University / nathanrwells@Ksu.edu
3. Asya Dvorkin / Princeton University / advorkin@cs.princeton.edu
4. Matthew Ellis / University of British Columbia / matthew.ellis@ubc.ca
5. Matthew West / UNC Charlotte / mwest53@charlotte.edu
6. Dan Bongert / UW Madison L&S SEO / dbongert@ssc.wisc.edu
7. Hemanth Bandi / University of Minnesota / bandi045@umn.edu
8. Nick Eggleston / Kansas State University / njeggleston@ksu.edu
9. Kurt Roberts / University of Cincinnati / Kurt.Roberts@uc.edu
10. Mike Robbert / NSF NCAR / mrobbert@ucar.edu
11. Ryan Cox / BYU / ryan_cox@byu.edu
12. Jim Leous / Consultant / jim.leous@gmail.com
13. Maxime Boissonneault / (Université Laval/Calcul Québec/Digital Research Alliance of Canada / maxime.boissonneault@calculquebec.ca)
14. Jay Sundu / UC Berkeley / jsundu@berkeley.edu
15. Bren Barker, Research Computing Center, University of Chicago, bbarker@uchicago.edu
16. Mike Carnegie / Penn State / mzc5001@psu.edu
17. Daniel Lucio / NC State / dalucio@ncsu.edu
18. Matthew Lambert / University of Tennessee / mlambe28@utk.edu
19. Ben Nickell - Idaho National Laboratory / ben.nickell@inl.gov
20. Davide Del Vento / Quantinuum / delvento@gmail.com
21. Brian Vanderwende / Quantinnum / brian.vanderwende@quantinuum.com

22. Sajesh Singh / American Museum of Natural History / ssingh@amnh.org
23. Ryan Thomson / University of British Columbia / ryan.thomson@ubc.ca
24. Damon Armour / NC State University / damon_armour@ncsu.edu
25. Michael Ewan / Portland State University / mewan@pdx.edu
26. Stephanie Heidemann | Internet2 | sheidemann-ctr@internet2.edu
27. Steve Bailey / National Institutes of Health / steve.bailey@nih.gov
28. Stephen MacDonald / UBC / Faculty of Science / stephen.macdonald@ubc.ca
29. Zoe Braiterman / Independent / braiterman.z@gmail.com
30. Alex Ptak / University of Virginia, Research Computing / ptak@virginia.edu
31. Torey Battelle / Arizona State University / tbattell@asu.edu
32. Nick Wehrheim / NSF NCAR / nickw@ucar.edu
33. Michele Co / University of Virginia, Research Computing / mc2zk@virginia.edu
34. Michael Peterson / NC State / michael_peterson@ncsu.edu
35. Ben Eisenbraun / Harvard Medical School / bene@hkl.hms.harvard.edu
36. Warren Frame / Harvard FAS Research Computing / wframe@g.harvard.edu
37. Jessica Galo/UBC/jessica.galo@ubc.ca
38. Ross Mickens / PSU/ rlm6137@psu.edu
39. Wade Klaver / UBC / wade.klaver@ubc.ca
40. Katia Bulekova / Boston University / ktrn@bu.edu
41. Vani Walvekar /Saint Louis University / vani.walvekar@health.slu.edu
42. Michael Walker / Texas A&M University / michaelwalker@tamu.edu
43. Kim Wilkins / University of Nevada Reno / kwilkins@unr.edu
44. Mark Hahn / McMaster University & Digital Research Alliance of Canada / hahn@sharcnet.ca
45. Kenneth Hoste / Ghent University (Belgium) / kenneth.hoste@ugent.be
46. Scott Goethals / Vanderbilt ACCRE / scott.goethals@vanderbilt.edu
47. Adam Focht / Penn State University / abf123@psu.edu
48.
49.
50.
51.
52.
53.
54.
55.

Call Notes:

- From chat: CopyFail exploit - https://www.kodemsecurity.com/resources/cve-2026-31431-copy-fail-linux-kernel-lpe-breakdown-and-remediation-runbook
- These seem to be becoming more common. Also, vulnerabilities that require very little knowledge to exploit, on systems with many untrusted users, seem to be more common.
- Because it was HPC, we had to take the lead and let our SOC help because we're more familiar.
- How do you triage these vulnerabilities? We have a variety of institutions that might be a single FTE vs. large research institutions with many staff/security staff members. If this is going to be a particular problem, can we leverage CaRCC or groups of small centers to share info? How do we share/instantiate this knowledge going forward? How do we get tools out there? In CA, we have a system in place for doing this. Also, SIG-HPC Slack has been invaluable.
- If there's an exploit without a fix yet, do you take these systems down?
- From chat: Linus Torvalds comments about dealing with the volume of emails & tickets on the Linux kernel - https://www.youtube.com/watch?v=4_x0USuQ9Ss
- Before we were able to contain the "blast radius" of the exploit, some of these vulnerabilities used our networks to move through the system.
- I think we need to be better at communicating the "Why?" behind system access blocks without giving away too much to users.
- From chat: I do recommend Daniel Stenberg's post about Mythos and his experience in maintaining Curl: https://daniel.haxx.se/blog/2026/05/11/mythos-finds-a-curl-vulnerability/
- Does the extra visibility of the AI and vulnerabilities explain to the users why these vulnerabilities are much more common?
- Some provide a Status Page to let the users know what's going on. What do people use for this?
    - Recommendation: Don't use your own infrastructure for this. This is where you might want to use cloud infrastructure or partner institutions.
    - OnDemand login page
    - Sometimes we respond with a canned email. Not always nice, but sometimes necessary.
- Do users need to be trained? Is this something that's covered in onboarding? Not really.
- We've been trying to train our users if something isn't covered, put a ticket in.
- During these problems, we send an email blast out to all users with links to the Status Page.
- When I train new admins, I always tell them NOT to reply using your individual email, rather through the ticket system.
- What is your relationship with the IT Security Team?
    - Very good, but we're always the group that's running outlier systems, one-offs
    - They often don't understand our operation, but we have regular meetings and a liaison to the Security org.
    - With the Federal system, we have Binding Operational Directives (BODs) that specify deadlines to patch different levels of vulnerabilities. We follow NIST 800-34.
- We have a class of user-run software, generative LLMs to write code, with very little understanding on the part of the user how it works, which can create new problems.
    - Does it really change our security posture? Can we use containers to restrict the "splash radius" of some of the user-related problems?

    - Banning VSCode? We know that users are going to run it.
- Advice:
    - Stop using the Cluster as your own laptop.
    - Lots of places are pursuing a persistent remote desktop
    - What do you need to know about the Linux kernel? Kernel development? Kernel module management? “Module jails” are getting more common, but are really aimed at the desktop environment. Will an HPC version of this evolve?
- How are people feeling? How are you dealing with burnout?
- Advocate for hiring more people to help manage and maintain our system, especially as these systems get more complex.
    - Need to talk to our funders? Why do we need more people?
    - Do we need to help our leadership understand the seriousness (or lack thereof) of the vulnerabilities and which ones are more urgent than others?

Upcoming Presentation Plans:

-

Suggest future topics for a Systems-Facing call (Feel free to add one!):

-