Responses to Vulnerability Notification by Security Companies

or: Why is this CVSS so low?
Greetings!

Andrew Ferbert
Platform Services Manager
San Diego Supercomputer Center

dferbert@sdsc.edu
My team doesn’t do “security research”
Once upon a time…
...we found a security problem before buying...
...and...
Company A:

- gave us lip service
- published a questionable CVSS score
- didn’t let us talk to engineering
- mitigated exactly how we said not to
Company A:

- gave us lip service
- published a questionable CVSS score
- didn’t let us talk to engineering
- mitigated exactly how we said not to
- announced there was a vulnerability
The next time, we bought the product THEN found a security problem
Company B:

- understood the impact
- gave constant feedback
- allowed us to discuss with engineering
- gave us pre-release code to verify
Company B:
- understood the impact
- gave constant feedback
- allowed us to talk to engineering
- gave us pre-release code to verify
- only mentioned vuln on current-customer support page
TL;DR

Push vendors to do better

Leverage your community (safely)

Keep looking