James Chad Ballay

The three specifically asked for:

* National Cyber Awareness System (<https://www.us-cert.gov/ncas>)
* Common Vulnerabilities and Exposures (<https://cve.mitre.org/>)
* SANS Internet Storm Center (<https://isc.sans.edu/>)

For my current role I narrow the focus down to the techstack I support but most of the time I don’t know to go check them until my vendor partner let’s us know about an incoming patch

* Red Hat <https://access.redhat.com/security/security-updates/>
* Tomcat <https://tomcat.apache.org/security-8.html>
* IBM MQ & IBM Informix <https://www.ibm.com/blogs/psirt/>

The pace of when a vulnerability is discovered to how quickly it can propagate boggles the mind.

Diversifying the software/hardware install base isn’t the answer since human support man hours don’t scale. For instances we can barely maintain a single team to provide Messaging as a Service at my workplace. There is no way to scale that to being 4 or 5 or 10 different messaging tech stacks. Then multiply that across every other component in the tech stack. Or even industry wide. This leaves the environment horrendously monocultured. Once an exploit is released it literally has chance of impacting large double-digit percentages of the install base due to this.

Once a compromise is widely published it will never go away. The libraries of CVE’s for previous versions of software products never gets smaller. The storage of this collected information is trivial. It is redundant and freely accessible. The bell truly cannot be unrung. I powered down my last AIX 4.3 server 5 years ago. I and most of the industry have collectively forgotten much of how to support this version. But at any point an AIX 4.3 box shows up as a target, every exploit previously disclosed can be tried in the hopes of the patching being behind on that server.

Automation takes those two previous facts and ramps up the pace. Faster than any human admin could ever react the time between a simple probing of your firewall can escalate to ring after ring of your defense in depth failing. We truly have to work smarter rather than harder since humans do not scale like computers do.

These early warning systems for disseminating threat vectors are critical in decreasing the window of opportunity for bad actors to attack. Individuals and companies still must act upon these alerts. Either by shifting security patches and automated testing to the left of the build process. But a coordinated early warning system is the first step and therefore the most critical step.