CYBER SAFETY REVIEW BOARD

CSRB REVIEW: DECEMBER 2021 LOG4J EVENT

Key Findings and Recommendations

Summary and Key Findings

The Department of Homeland Security (DHS) established the Cyber Safety Review Board (CSRB) in February 2022 to review significant cybersecurity events so that government, industry, and the broader cybersecurity community can better protect our nation's networks and infrastructure. The CSRB is an unprecedented public-private initiative that brings together government and industry leaders to identify lessons learned from significant incidents and deliver strategic, actionable recommendations. Robert Silvers, Under Secretary for Policy at DHS, serves as Chair of the CSRB, and Heather Adkins, Vice President, Security Engineering at Google, serves as Deputy Chair.

The CSRB's inaugural review was of the events surrounding the December 2021 disclosure of a vulnerability in Log4j. Log4j is a popular, open source, and Java-based logging framework, incorporated into thousands of other software packages, that collects and manages information about system activity. The discovery of the Log4j vulnerability led to one of the most intensive cybersecurity community responses in history.

During this inaugural review, the CSRB engaged with nearly 80 organizations and individuals to gather insights into the Log4j event, inform findings, and develop actionable recommendations to prevent and respond more effectively to future incidents. Highlights of the Board's findings include:

- Log4j is one of the most serious software vulnerabilities in history. Log4j is an "endemic vulnerability" and unpatched versions of Log4j will remain in systems for years to come, perhaps a decade or longer. The event is not over. Risk remains and network defenders must stay vigilant.
- Many companies could not quickly identify where in their environments they had vulnerable code, revealing opportunities to increase software transparency and capacity to respond quickly to newly-discovered vulnerabilities.
- The Board raised significant concerns regarding the People's Republic of China (PRC) government regulations governing the disclosure of software vulnerabilities. The Board found that the PRC government could use these regulations to get early access to newly-discovered vulnerabilities that it can then exploit for its own malicious purposes.
- This event highlighted security risks unique to the thinly-resourced, volunteer-led open source software community. Industry and the federal government must commit more resources to supporting open source software security.
- Software developers often do not have access to training programs in secure software development practices. The Board recommended that universities and community colleges should require a cybersecurity component for all computer science degrees and certifications.

The Cyber Safety Review Board was established by the U.S. Department of Homeland Security as directed in President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity. The CSRB is responsible for conducting authoritative reviews and assessments of significant cyber events. Half of its members are senior U.S. government officials, and half are luminaries from the private sector cybersecurity community.

Recommendations

Address Continued Risks of Log4j

Continued vigilance in addressing Log4j vulnerabilities for the long term

1. Organizations should be prepared to address Log4j vulnerabilities for years to come.
2. Organizations should continue to report (and escalate) observations of Log4j exploitation.
3. CISA should expand its capability to develop, coordinate, and publish authoritative cyber risk information.
4. Federal and state regulators should drive implementation of CISA guidance through their own regulatory authorities.

Drive Existing Best Practices

Adopt industry-accepted practices and standards for vulnerability management and security hygiene

5. Organizations should invest in capabilities to identify vulnerable systems.
6. Develop the capacity to maintain an accurate information technology asset and application inventory.
7. Organizations should have a documented vulnerability response program.
8. Organizations should have a documented vulnerability disclosure and handling process.
9. Software developers and maintainers should implement secure software practices.

Build a Better Software Ecosystem

Drive a transformation in the software ecosystem to move to a proactive model of vulnerability management

10. Open source software developers should participate in community-based security initiatives.
11. Invest in training software developers in secure software development.
12. Improve Software Bill of Materials tooling and adoptability.
13. Increase investments in open source software security.
14. Pilot open source software maintenance support for critical services.

Investments in the Future

Pursue cultural and technological shifts necessary to solve for the nation's digital security for the long run

15. Explore a baseline requirement for software transparency for federal government vendors.
16. Examine the efficacy of a Cyber Safety Reporting System.
17. Explore the feasibility of establishing a Software Security Risk Assessment Center of Excellence.
18. Study the incentive structures required to build secure software.
19. Establish a government-coordinated working group to improve identification of software with known vulnerabilities.