Debugging the Decade: 
10 years of Product Incident Response at Adobe

David Lenoe – Director, Product & Services Security
Tom Cignarella – Director, Security Coordination Center
Intro

Dave

PSIRT & ASSET

Tom Cignarella

Security Coordination Center
aka CERT

Security Monitoring (SOC)
Incident Response (IR)
Background
10 years of ASSET

(Not ASSES)
Adobe
Adobe web services vulnerability disclosure program
adobe.com/security • Adobe Security

Guidelines

This disclosure program is limited to security vulnerabilities in web applications owned by Adobe. All vulnerabilities affecting Adobe desktop products (ex. Flash Player and Adobe Reader), or enterprise on-premise solutions should be reported via email to the Product Security Incident Response Team [PSIRT@adobe.com] (PGP key available here).

Eligible Vulnerabilities

We encourage the coordinated disclosure of the following eligible web application vulnerabilities:

- Cross-site scripting
- Cross-site request forgery in a privileged context
- Server-side code execution
- Authentication or authorization flaws
- Injection Vulnerabilities
- Directory Traversal
- Information Disclosure
- Significant Security Misconfiguration

To receive credit, you must be the first reporter of a vulnerability and provide us a reasonable amount of time to remediate before publicly disclosing. When submitting a vulnerability, please provide concise steps to reproduce that are easily understood.

Program Exclusions

See all hackers
What’s a 0-day exploit?
Adobe Reader JBIG2 vulnerability - 2008
JBIG2 vs. HackingTeam timeline

- JBIG 0-day – 2009
- HackingTeam 0-day – 2015

23X Faster
Lessons Learned

Over the past 10 years there are several lessons learned that we’d like to share with you…
VS.
Lesson 1: Patching is painful
Patching is painful – Pro Tip

• Be prepared!
  • Have a plan in place
  • Test it out
  • Push the limits
Lesson 2: Highlight on Hygiene
Lesson 3: Spotting the Signal in the Noise
Lesson 3: Spotting the Signal in the Noise
Spotting the Signal in the Noise – Pro Tip

• Shift your perspective
  • Doesn’t have to be trolling through logs
• Anomaly detection
• Focus on chatter outside the firewall
Lesson 4: Cultivate Your Community
Lesson 4: Cultivate Your Community

- Pen test for Adobe service
- Evaluation of crowd-sourced pen test service
- Evaluation of web app security service

3 birds: 1 stone
Cultivate Your Community – Pro Tip

• Shall we play a game?
  • Gamify!
• Talk to your Frenemies
  • All in this together
Lesson 5: Silos are Suboptimal
Lesson 6: Good Hiring
Lesson 7: Keeping an even keel

Keep Calm and Be Nice
Lesson 8 - Post-mortems rule

“Those that do not learn from history are doomed to repeat it”

George Santayana
Lesson 9: Don’t take it personally

Don’t Take It Personally
Lesson 10: Never waste a crisis

“People only accept change when they are faced with necessity and only recognize necessity when a crisis is upon them.”

— Jean Monet
Lesson 11: PSIRT versus CERT?

- PSIRT – Has deeper hooks into the dev community
- PSIRT – more externally facing
- CERT – starting to be become more externally facing (threat intel)

Communication is key for both
- PSIRT to researchers
- CERT to internal stakeholders and eventually customers
Lesson 11: PSIRT AND CERT
Lesson Summary

1. Master patching
2. Have good hygiene
3. Control the signal to noise ratio
4. Cultivate the community
5. Tear down those silos
6. Careful with every person you hire
7. Remain calm
8. Learn from your mistakes
9. It’s not about you
10. Never waste a crisis
11. PSIRT and CERT must work together
Bonus Lesson: Always keep an eye on the future...
Everything is connected
Forbes 100 Companies with Vulnerability Disclosure Programs

13% have disclosure programs

87% do not have disclosure programs

94% of the companies in the Forbes Global 2000 do NOT have a known vulnerability disclosure program.

FORBES 100 RANKING
9 General Electric
12 Apple
22 Verizon Communication
25 Microsoft
27 AT&T
39 Google
40 Vodafone
44 IBM
70 Deutsche Telekom
76 Cisco Systems
88 Oracle
92 ING Group
97 Hewlett-Packard

TECHNOLOGY  TELECOMMUNICATIONS  FINANCIAL SERVICES
"Have an effective process to receive and address security vulnerability reports. Consider an effective channel (for example, security@yourcompany.com) for receiving reports for your security staff."

- Lessons learned from FTC cases. FTC, June 2015
Thank You
Instruction Slide

• Please **do not delete** the title slide.
• You are **not required** to use this template.
• You are welcome to include your organization’s logo/brand on the presentation title page.
• You are also welcome to adjust the location of your logo as long as it does not overlap/touch the FIRST logo.
• Your slides must be reviewed prior to your presentation by the FIRST Program Chair and Committee.