Didn't You Hear Me?
Towards More Successful Web Vulnerability Notifications

Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow
Motivation and Research Questions

- Prior works in this area had limited impact
  - Low fix rates
  - Main issue: few administrators reached

- Our work: understand why notifications did not perform better and determine improvements
  - Message format/tone
  - High-effort channels
Study Setup
Types of Disclosed Issues

- Well-known vulnerabilities for WordPress (14,815 domains, Top 1M)
  - Two Cross-Site Scripting Flaws (CVE-2016-4566, CVE-2016-4567)
  - determined by hash values of vulnerable Flash files

- Misconfigured Git repositories (9,721 domains, Top 1M)
  - Checked presence and format of .git/config
  - Removed known public repositories (based on hash of last commit)

- Publicly accessible core dumps (790 domains, Top 1M)
  - excluded later in the experiment
  - one hoster responsible for 30% of affected sites
Different Types of Notifications

- **Plain text emails**
  - Real name sender (**Plain**), "Vulnerability Notification" sender (**Mailbot**), Signed emails (**S/MIME**)  

- **HTML emails**
  - HTML with all information included (**HTML**), HTML with externally linked logo (**Tracking**)  

- **Friendly tone**
  - Merely information that some flaws was detected  
  - asked for right contact to provide more info
Notification Procedure

- Used only directly available channels
  - security/abuse/webmaster/info@domain.com, WHOIS abuse contact

- Split up data set of vulnerable domains into seven groups
  - different messages and control group

- Bi-weekly emails
  - February 3rd, February 17th, March 3rd
Results of our Notification
Remediation Overview

**Git**

Significant improvement for all groups

Significant improvement only for Mailbot

**WordPress**
Access Reports over Time

Friendly performed best for delivering report

Plain, Mailbot, S/MIME almost same

HTML Emails yielded least hits on reports

Git

Wordpress
Insights from Tracking Analysis
Spam Filtering

- Analyzed fraction of tracked emails per provider
  - Removed bounces first
  - Google, Microsoft-hosted (business), all other providers

- Assumption: inherent email access levels do not vary

- Drastic difference between providers
  - likely due to Google's spam filters
Read emails to viewed report to fixed issues

- **Emails read**
  - Git: 40%
  - WordPress: 20%

- **Email to Report**
  - Git: 20%
  - WordPress: 40%

- **Tracked and fixed domains**
  - Git: 75%
  - WordPress: 25%

---

Ben Stock - NDSS 2018 - Didn't You Hear Me? Towards More Successful Web Vulnerability Notifications
Parameters to the Success of a Notification Campaign

- Initial Notification Messages
  - Email Reading Rate
  - Unknown Spam?
    - Opened by Recipient
    - Bounced
  - Spam?
    - Unknown
      - Opened by Recipient
      - Bounced
    - Issue fixed
      - Report Read
        - Issue fixed
          - Git
            - Report Read
              - WordPress
                - Report Read
                  - Issue fixed
Manual Notification
Manual Notification - Channels and Availability

- Randomly sampled 970 unfixed domains
  - only domains without previous viewed reports

- Manually checked each site for contact info
  - considered postal, email, forms, social media, and phone
  - ~90% had at least one

- Randomly assigned channel to each domain
  - to avoid bias, availability of channel not considered
  - only 364/970 domains could be contacted
Hi, this is Sponser, I am a researcher at Saarland University in Germany. I have found a vulnerability on your website. I would like to disclose it.

Are you the right person?

Yes

Can you give me your email address to disclose this?

Yes

Bye

No

Do you speak EN? Do you understand EN?

Yes

Bye

No

Can you connect me to that person?

Yes

Bye

No

Can you give my email address to that person? (notify@cispa.saarland)

Yes

Bye

No

I don't trust your accent

No
Manual Notification - Results

- 60 hours of manual work
  - 40 hours for contact lookup
  - 20 hours for notifications

- Reaching
  - Notable improvement for Git
  - Small improvement for WordPress

- Fix: no improvements

- Bias needs to be considered
Quo Vadis Vulnerability Notifications

• Better Delivery Mechanisms
  • security@ bounced for 85% of all domains
  • Google's spam filter likely had significant impact on success

• Increasing Trust in Notifications
  • only between 1/6 and 1/4 followed up on our information
  • prior work with Search Console yielded 80% reactions

• Tailored Notifications
  • low fix rates for WordPress indicate lack of proper understanding
Different Types of Notifications

- Plain text emails
  - Real name sender (Plain), "Vulnerability Notification" sender (Mailbot)
  - Signed emails (S/MIME)

- HTML emails
  - HTML with all information included (HTML)
  - HTML with externally linked logo (Tracking)

- Friendly tone
  - Merely information that some flaws was detected
  - asked for right contact to provide more info

Parameters to the Success of a Notification Campaign

- 60 hours of manual work
  - 40 hours for contact lookup
  - 10 hours for calls
  - 5 hours mailers
  - 5 hours forms/social media

- Reaching: Notable improvement for Git, small improvement for WordPress

- Fix: no improvements

More info (including survey) can be found in our paper.

Thanks!