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
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
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
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)
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)
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**)
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

---

Hello,

I am a security researcher at the Center for IT-Security, Privacy and Accountability at Saarland University, Germany. I have found a vulnerability in your site domain.com. I would like to disclose the vulnerability to the correct contact. Could you please point me to that person or confirm that this is you?

Thank you and best regards,

Ben

---

Dr.-Ing. Ben Stock
Center for IT-Security, Privacy and Accountability (CISPA)
Saarland University
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

![Graph showing Remediation Overview over time](image_url)
Remediation Overview

Significant improvement for all groups

Git
Remediation Overview

Significant improvement for all groups

**Git**

**WordPress**
Remediation Overview

Significant improvement for all groups

Significant improvement only for Mailbot

Git

WordPress
Access Reports over Time

Git

WordPress
Access Reports over Time

Friendly performed best for delivering report
Access Reports over Time

Friendly performed best for delivering report

Plain, Mailbot, S/MIME almost same
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

![Tracked domains chart]

- Tracked domains: [Google, Microsoft, Others]
Read emails to viewed report to fixed issues

![Emails read chart]

- Git: 40%
- WordPress: 20%

Read Emails
Read emails to viewed report to fixed issues

Emails read

<table>
<thead>
<tr>
<th></th>
<th>Git</th>
<th>WordPress</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Email to Report

<table>
<thead>
<tr>
<th></th>
<th>Git</th>
<th>WordPress</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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: Report viewed: 75%, Report not viewed: 25%
Read emails to viewed report to fixed issues

**Emails read**

- **0 %** for Git
- **40 %** for WordPress

**Email to Report**

- **20 %** for Git
- **40 %** for WordPress

**Tracked and fixed domains**

- **75 %** for Git
- **0 %** for WordPress

**Conversion**

- **0 %** for Git
- **50 %** for WordPress

**Report viewed**

- **0 %** for Git
- **25 %** for WordPress

**Report not viewed**

- **100 %** for Git
- **100 %** for WordPress

**Control**

- **0 %** for Git
- **0 %** for WordPress
Parameters to the Success of a Notification Campaign

Initial Notification Messages
Parameters to the Success of a Notification Campaign

Initial Notification Messages

- Opened by Recipient
- Unknown Spam?
- Bounced
Parameters to the Success of a Notification Campaign

Initial Notification Messages

- Opened by Recipient
  - Unknown Spam?
    - Bounced

Report Read

Git

Wordpress

Report Read
Parameters to the Success of a Notification Campaign

Parameters to the Success of a Notification Campaign

Email Reading Rate

Initial Notification Messages

Opened by Recipient

Unknown Spam?

Bounced

Report Read

Report Read

Issue fixed

Git

WordPress
Parameters to the Success of a Notification Campaign

Initial Notification Messages

- Email Reading Rate
  - Opened by Recipient
    - Unknown Spam?
      - Bounced

- Awareness Raising Rate
  - Report Read
    - Issue fixed
  - Git
  - WordPress
    - Report Read

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

Opened by Recipient

Unknown Spam?

Bounced

Awareness Raising Rate

Report Read

Git

WordPress

Issue fixed

Aware-to-fix Rate

Report Read
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
Manual Notification - Roadblocks
Hi, this is Sperson, I am a researcher at Saarland University in Germany. I have found a vulnerability on your website. I would like to disclose it.

Do you speak EN? Do you understand EN?

Are you the right person?

Can you connect me to that person?

Can you give me your email address to disclose this?

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

Yes

Yes

Yes

Yes

Yes

Yes

No

No

No

No

Bye

Bye

Bye

Bye
Hi, this is Sperson. I am a researcher at Saarland University, Germany.
I have found a vulnerability on your website.
I would like to disclose it.

Do you speak EN?
Do you understand EN?

Are you the right person?

Can you connect me to that person?

Can you give me your email address to disclose this?

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

Bye

Bye

Bye
Hi, this is $person, 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?

Can you connect me to that person?

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

No

Can you give me your email address to disclose this?

Yes

Bye

Bye

I don't trust your accent

Do you speak EN? Do you understand EN?
Do you speak EN? Do you understand EN?

Hi, this is Speron, 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?

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

I don't trust your accent
Manual Notification - Results
Manual Notification - Results

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

Viewed Reports

<table>
<thead>
<tr>
<th>Method</th>
<th>Git (%)</th>
<th>WordPress (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Postal</td>
<td>20</td>
<td>15</td>
</tr>
<tr>
<td>Email</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Web forms</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Social Media</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Phone</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Best Automated</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
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
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
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 were detected
  - asked for right contact to provide more info

Access Reports over Time

- Friendly performed best for showing report
- Plain, Mailbot, S/MIME almost same
- HTML Email process best, hits on reports

Git

WordPress
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 were detected
  - asked for right contact to provide more info

Access Reports over Time

Parameters to the Success of a Notification Campaign
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 were detected
  - asked for right contact to provide more info

Access Reports over Time

Parameters to the Success of a Notification Campaign

- Initial Notification Messages
  - Opened by Recipient
  - Unknown Spam?
  - Bounced

- Email Reading Rate

- Awareness Rating

- Avoid to Fix Rate

- Viewed Reports

- Fixed Domains

Manual Notification - Results

- 60 hours of manual work
  - 40 hours for contact lookup
  - 10 hours for calls
  - 5 hours letters
  - 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.
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 were detected
  - asked for right contact to provide more info

Parameters to the Success of a Notification Campaign

- Initial Notification Messages
  - Opened by Recipient
  - Unknown Spam?
  - Bounced

- Email Reading Rate

- Awareness Rating

Access Reports over Time

- Git
- WordPress

Manual Notification - Results

- 60 hours of manual work
  - 40 hours for contact lookup
  - 10 hours for calls
  - 5 hours for letters
  - 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.
Backup Slides
Ethical considerations

• Observed ethical practices in our study
  • non-intrusive tests for flaws
  • opt-out option for notified parties
  • used "blacklist" from previous work
Ethical considerations

- Observed ethical practices in our study
  - non-intrusive tests for flaws
  - opt-out option for notified parties
  - used "blacklist" from previous work

- Collected least possible information
  - no PII stored for recipients
    - merely bit "read email"/"viewed report"
  - no data retrieved from Git repositories
    - introduced chance of false positive
Survey and Feedback Insights

- Best contact: WHOIS technical (not abuse)

- Trust in information remains biggest issue
  - provide verifiable information
    - Saarland University not known in the US (our bad! ;-))
  - S/MIME did not make a difference
  - scammers are doing similar "notifications"

- Few replies only for manual feedback
  - 6/15 WordPress owners did not care
  - Problems reappeared (reasons unclear)
Language Comparisons (Git)

- **German**
- **English**
- **Spanish**
- **Japanese**
- **Russian**
Language Comparisons (WordPress)