THE SKY IS FALLING!
RESPONDING RATIONALLY TO HEADLINE VULNERABILITIES

Gill Langston
Director, Product Management
Qualys, Inc.
Why are we here

- Our emergency response playbook has solved all of our problems
Why are we here

- Our emergency response playbook has solved all of our problems
- This job is pretty boring these days since we are ahead of the curve
Why are we here

- Our emergency response playbook has solved all of our problems
- This job is pretty boring these days since we are ahead of the curve
- When a high profile vulnerability comes along, it makes my day
Why are we here

- Our emergency response playbook has solved all of our problems
- This job is pretty boring these days since we are ahead of the curve
- When a high profile vulnerability comes along, it makes my day

NO?
Today’s news cycle

- Executive visibility
- High noise level vs. what's important
- Public accountability
- Need a better plan for response
If You Have Windows, Update It Right Now To Keep This Massive Hack Out

More than 150 countries across the world are being targeted in what cybersecurity experts say may be the biggest ransomware attack ever observed.

Posted on May 12, 2017, at 4:48 p.m.

Sheera Frenkel
BuzzFeed News Reporter

They don’t go away on their own!

Someone else’s problem
Discussion

- Review of anonymized, aggregated Qualys customer detections
- Response challenges based on patching behavior trends
- Real-world best practices based on analysis of remediation(s)
WannaCry – notable info

- High risk issue
- Highly publicized (NSA/Shadow Brokers hack)
- Mitigations – Risky

CVSS Severity (version 3.0):
- CVSS v3 Base Score: 8.1 High
  - Impact Score: 5.9
  - Exploitability Score: 2.2

CVSS Version 3 Metrics:
- Attack Vector (AV): Network
- Attack Complexity (AC): High
- Privileges Required (PR): None
- User Interaction (UI): None
  - Scope (S): Unchanged
  - Confidentiality (C): High
  - Integrity (I): High
  - Availability (A): High
WannaCry timeline

- **Mar 14, 2017**: MS17-010 released (CVEs also published)
- **Apr 14, 2017**: Shadow Brokers releases exploit code
- **May 10, 2017**: WannaCry v1 attacks begin using EternalBlue exploit
- **May 12, 2017**: WannaCry v2 attacks explode
- **Jun 27, 2017**: New Petya malware outbreak using same exploit
WannaCry detections

MS17-010 Detections

Thousands


- MS17-010 released
- Shadow Brokers
- WannaCry v1 attacks
- WannaCry v2 attacks
- New Petya
WannaCry takeaways – why we struggled

- Identification of all at-risk assets was slow

- All issues sometimes treated the same by ITOps teams

- Widespread user participation requirement created delays in remediation
  - If they don’t know its critical, complacency sets in
WannaCry Impact

- Large Organizations infected
  - Stayed present in news cycle

- Panic to resolve issue from top-down
  - Identify vulnerable assets
  - Determine fixes
  - Complete patching cycle

- Reinforced need to improve patching cycles
Struts – notable info

- High risk
- Easy to exploit

CVSS Severity (version 3.0):

- CVSS v3 Base Score: 10.0 Critical
- Impact Score: 6.0
- Exploitability Score: 3.9

CVSS Version 3 Metrics:

- Attack Vector (AV): Network
- Attack Complexity (AC): Low
- Privileges Required (PR): None
- User Interaction (UI): None
- Scope (S): Changed
- Confidentiality (C): High
- Integrity (I): High
- Availability (A): High

Struts timeline

Mar 6, 2017
- CVE-2017-5638 released
- Updated libraries released
- Exploit available

May 13, 2017
- Reported as date of Equifax breach

July 29, 2017
- Reported discovery date of breach

Sep 7, 2017
- Breach reported publicly
Struts Vulnerability

Struts Web Application Scans

- CVE-2017-5638 released
- Updated libraries released
- Exploit available

- Equifax breach
- Discovery date
- Reported publicly

RSA Conference 2018
Struts takeaways – why we struggled

- Long delays in remediating web applications

- Not easily fixed
  - Not always as simple as pushing a patch
  - Application rebuild
  - Testing cycles
Struts Impact

- Highly public data breach
  - Delay in updating web application was the cause

- Reinforces need for mitigations (Web Application Firewall, filtering rules)
Meltdown/Spectre— notable info

- Requires access to machine
  - Could be delivered via multi-stage attack
  - Few-to-no exploits available

- Mitigation – Patch was a mitigation
  - Also ensure layered security is up-to-date

---

**CVSS v3.0 Severity and Metrics:**

- **Base Score:** 5.6 MEDIUM
- **Vector:** AV:L/AC:H/PR:L/UI:N/S:C/H:I:N/A:N (V3 legend)
- **Impact Score:** 4.0
- **Exploitability Score:** 1.1

**Attack Vector (AV):** Local
**Attack Complexity (AC):** High
**Privileges Required (PR):** Low
**User Interaction (UI):** None
**Scope (S):** Changed
**Confidentiality (C):** High
**Integrity (I):** None
**Availability (A):** None
Meltdown/Spectre timeline

- **Jan 3, 2018**: Vulnerabilities published
- **Jan 3, 2018**: MS releases emergency update
- **Jan 22, 2018**: Intel recommends updates be halted
- **Jan 27, 2018**: MS “patches the patch”
- **Feb 28, 2018**: MS releases new microcode updates
Intel recommends updates halted
MS releases new microcode updates
MS “patches the patch”

Vulnerabilities published
MS releases emergency update

Meltdown Detections

Meltdown

0 500000 1000000 1500000 2000000 2500000 3000000 3500000
Meltdown/Spectre takeaways – why we struggled

- No fixes, only mitigation patches
Meltdown/Spectre takeaways – why we struggled

- No fixes, only mitigation patches
- Every OS patch had a downside
Meltdown/Spectre takeaways – why we struggled

- No fixes, only mitigation patches
- Every OS patch had a downside
- Affected handling of memory
Meltdown/Spectre takeaways – why we struggled

- No fixes, only mitigation patches
- Every OS patch had a downside
- Affected handling of memory
- Tons of caveats and risk
Meltdown/Spectre Impact

- Panic – so many systems affected

- Fix caused major issues
  - Generated a lot of churn in IT orgs

- Reinforces need to....wait?
Overall takeaways

- Leaving high profile vulnerabilities to the current cycle doesn’t work
- Not all newsworthy vulnerabilities mean the same to you
- Sometimes the fix can be worse than waiting!
- Things can change quickly
- Lacking a thorough response plan can generate chaos
  - Internal pressure
  - External requests (is my data protected? Will business proceed normally?)
Put it all together

- Identify high-risk vulnerabilities - often
- Track the risk to your organization
- Determine best course of action (Remediate? Mitigate? Wait?)
- Decide when to communicate
- Update regularly
- Work the plan and improve
Get buy-in from teams (Executive, SecOps, DevOps, ITOps)
Build playbook together
Response plan elements

- Ensure all assets are identified
- Document the triggers
- Build communication plan
**Response plan elements**

<table>
<thead>
<tr>
<th>Prepare</th>
<th>React</th>
<th>Review</th>
<th>Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure all assets are identified</td>
<td>• Work the playbook</td>
<td>• Decide on Fix/Wait/Mitigate</td>
<td></td>
</tr>
<tr>
<td>• Document the triggers</td>
<td></td>
<td>• Communicate with your users</td>
<td></td>
</tr>
<tr>
<td>• Build communication plan</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Response plan elements

<table>
<thead>
<tr>
<th>Prepare</th>
<th>React</th>
<th>Review</th>
<th>Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure all assets are identified</td>
<td>• Work the playbook</td>
<td>• Retrospective</td>
<td></td>
</tr>
<tr>
<td>• Document the triggers</td>
<td>• Decide on Fix/Wait/Mitigate</td>
<td>• Identify areas to improve</td>
<td></td>
</tr>
<tr>
<td>• Build communication plan</td>
<td>• Communicate with your users</td>
<td>• Don’t get discouraged!</td>
<td></td>
</tr>
</tbody>
</table>

Prepare
- Ensure all assets are identified
- Document the triggers
- Build communication plan

React
- Work the playbook
- Decide on Fix/Wait/Mitigate
- Communicate with your users

Review
- Retrospective
- Identify areas to improve

Improve
- Don’t get discouraged!
### Response plan elements

<table>
<thead>
<tr>
<th>Prepare</th>
<th>React</th>
<th>Review</th>
<th>Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure all assets are identified</td>
<td>• Work the playbook</td>
<td>• Retrospective</td>
<td>• Work together to improve response</td>
</tr>
<tr>
<td>• Document the triggers</td>
<td>• Decide on Fix/Wait/Mitigate</td>
<td>• Identify areas to improve</td>
<td>• Modify the plan based on findings</td>
</tr>
<tr>
<td>• Build communication plan</td>
<td>• Communicate with your users</td>
<td>• Don’t get discouraged!</td>
<td>• Expand the plan to all high-severity vulnerabilities</td>
</tr>
</tbody>
</table>

Prepare

React

Review

Improve
#RSAC

## Communications

<table>
<thead>
<tr>
<th>Alert Users?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Mechanism</td>
<td>Email</td>
<td>Prompts</td>
</tr>
</tbody>
</table>

### Alert Details:

<table>
<thead>
<tr>
<th>External Comm?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Mechanism</td>
<td>Public Website</td>
<td>Social Media</td>
</tr>
</tbody>
</table>

### Actions

<table>
<thead>
<tr>
<th>Last Action:</th>
<th>Complete?</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Action:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CVE-2017-5754

**Threat**
- All Assets Identified? Yes ☐ No ☐
- Active Attack? Yes ☐ No ☐
- Vector
  - Remote ☐
  - Local ☐
  - Web ☐

**Vector Details:** Must have access to assets

**Fix Available?** Yes ☐ No ☐
**Fix Tested?** Yes ☐ No ☐
**Risks/Issues?** Yes ☐ No ☐

**Risk Details:** Performance issues, unexpected reboots.

**Mitigation Available?** Yes ☐ No ☐
**Mitigation Tested?** Yes ☐ No ☐
**Risks/Issues?** Yes ☐ No ☐

**Risk Details:**

---

**Recommendation**

**Current Recommendation:** Fix ☐ Wait ☐ Mitigate ☒

**Reason for Recommendation:**
*Patches known to cause issues. No active attacks.*
*Ensuring antivirus, web filters, and email filtering is up to date in case of multi stage attack*

**Trigger to Change Recommendation:**
*Active attack that could be triggered by user,*
*Confirmation that all issues with patches are resolved*

---

**Communications**

**Alert Users?** Yes ☐ No ☐
**Alert Mechanism**
- Email ☐
- Patching ☒
- Prompts ☐

**Alert Details:** None at this time

**External Comm?** Yes ☐ No ☐
**Alert Mechanism**
- Public Website ☐
- Social Media ☐
- Internal site ☐

**Alert Details:**

---

**Actions**

**Last Action:** Test Meltdown patches
**Complete?** Yes ☐ No ☐
**Next Action:** Monitor for changes in threat landscape
### CVE-2017-5754

**Threat**
- All Assets Identified? Yes No
- Active Attack? Yes No
- Vector
  - Remote
  - Local
  - Web
  - Multi-stage attack via email

**Vector Details:**
- Fix Available? Yes No
- Fix Tested? Yes No
- Risks/Issues? Yes No
  - Performance issues, unexpected reboots.

**Recommendation**
- Current Recommendation
  - Fix
  - Wait
  - Mitigate

**Reason for Recommendation:**
*Known attack using email and websites tricking users into downloading exploit. Recommending we deploy fixes for applications and browsers, and waiting on operating systems until issues are resolved.*

**Trigger to Change Recommendation:** none at this time

**Communications**
- Alert Users? Yes No
  - Alert Mechanism
    - Email
    - Patching Prompts
  - Alert Details:
    - Inform users of known threats and reinforce user training

- External Comm? Yes No
  - Alert Mechanism
    - Public Website
    - Social Media
    - Internal site
  - Alert Details:
    - Internal site with company response for copy/paste

**Actions**
- Last Action: Deployed patch to test group
- Complete? Yes No
- Next Action: Roll out patches to affected machines

**Mitigation Available?** Yes No
**Mitigation Tested?** Yes No
**Risks/Issues?** Yes No
**Risk Details:**
A rational response
Next Week

- Identify the stakeholders (SecOps, ITOps, Dev, Exec Team)
- Decide how you would document and share:
  - Business impact if you do nothing (Wait to see changes in landscape)
  - Business impact if you do something (Apply Fix OR Mitigation)
  - Triggers - monitor threat feeds for changes
- Decide on the KPIs – how would you measure success?

Next Quarter (or next event)

- Work the playbook
- Daily ‘stand-up’ during event
- Review with team and decide together
- Document each step of action plan

Next 6 months

- Measure success
- Identify where to improve
- Don’t get discouraged by early failures or delays
  - This is a process!
- Repeat
A rational response

- High-profile vulnerabilities are not going away
  - Relying on other teams to handle just won’t work

- More executive visibility = panic mode for teams
  - Help be the stabilizing force in reaction

- Methodical approach leads to rational response
THANK YOU!

Gill Langston - Director, Product Management
Qualys, Inc.