Managing Cloud Vulnerabilities

Angela Lindberg, SAP
April 4, 2019
4 Vancouver
6 Walldorf
10 Bangalore
Purpose and Agenda

Purpose
- Share experience handling customer cloud penetration reports
- Observations and challenges
- Engage in discussion, any insights, advice, best practices…

Proposed Agenda
- 30 minutes of presentation and sharing experience
- 15 minutes of discussion to share solutions or ideas to streamline process

References
Outcome new ideas
Customers moving from on-premise to Cloud: the benefits and security considerations
Cloud provides service, architecture and deployment models

Cloud Architecture - multitenant & single-tenant
Cloud security considerations

- Top consideration Security and Privacy
- Regulatory, compliance or audit requirements
- Request to audit = cloud pen-test
- Shared responsibility customer and Cloud provider
A new experience handling customer reported cloud vulnerabilities...
Cloud penetration testing approach and results

- Automated tools results may include:
  - high numbers of false positives
  - generic descriptions
  - lack details to validate
  - shared responsibility inside and outside the company
- Priority ratings
Findings reported

- All sorts of findings, not all are vulnerabilities
- Repeated findings customers test independently of each other
- Challenge cleanse report
- Solutions? knowledge base, or establish security expert for each cloud offering
Consumer service expectations

- Expectations vary from high to passive
- Review based on customer priority
- Common Vulnerability Scoring System (CVSS) not as important for Cloud - internally used to validate findings
- Service Level Agreement (SLAs) currently under review for cloud offerings
Communication role redefined

- Communication expands to a customer support role
- New skills required to manage expectations and ensure confidence
- Considerations secure communications – Non Disclosure Agreement (NDA)
- Tracking and reporting findings
Cloud areas review and remediation

- Engineers review full report
- Prioritize based on customer priority
- Create ticket in back end systems for validated findings
  – not linked to on-premise ticketing system
- Cloud and on-premise versions require co-ordination
- Cloud fix applied for all customers
## On-premise vs Cloud

<table>
<thead>
<tr>
<th>Subject</th>
<th>On-premise</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>External researchers</td>
<td>Customers and 3\textsuperscript{rd} party testers.</td>
</tr>
<tr>
<td>Types of issues reported</td>
<td>Most are verified vulnerabilities</td>
<td>A range of findings, not all are vulnerabilities.</td>
</tr>
<tr>
<td>Number of reported findings</td>
<td>Typically, one</td>
<td>Full report with multiple findings.</td>
</tr>
<tr>
<td>CVSS</td>
<td>Required</td>
<td>Customers provides priority rating. CVSS used internally on occasions to validate severity.</td>
</tr>
<tr>
<td>Patch released</td>
<td>Required</td>
<td>Not required. Fix typically released faster than on-premise to all Tenants. No patches. No customer action required.</td>
</tr>
</tbody>
</table>
Cloud process continues to evolve
Thank you.

Contact information:

**Angela Lindberg**  
Security Response Analyst
References

- https://nmap.org/
- https://portswigger.net/burp
- https://www.tenable.com/products/nessus/nessus-professional