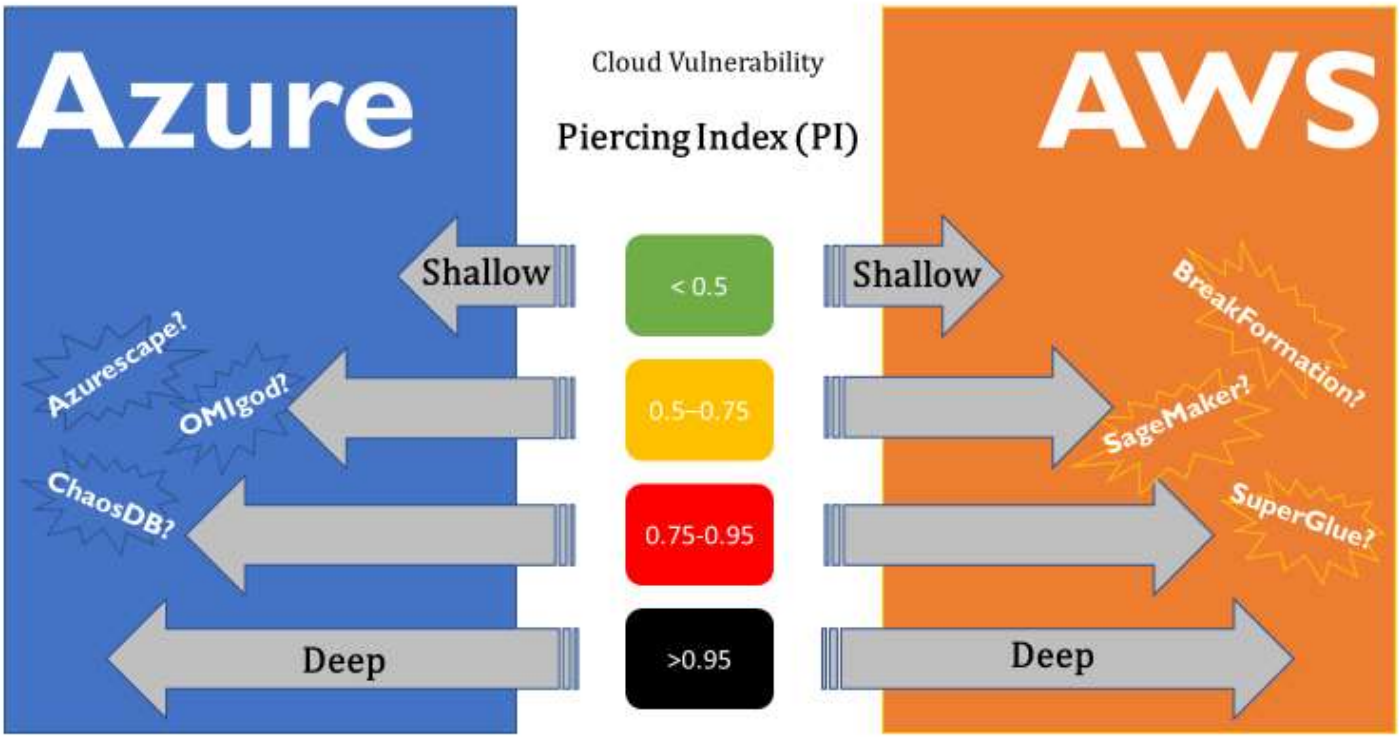
The Piercing Index

A scoring system for assessing Cloud provider security vulnerabilities

Author: Christophe PARISEL

Version: 1.5, December 29, 2022

Permalink:
https://github.com/labyrinthinesecurity/cloudVulnerabilities/tree/main/PiercingIndex.pdf



How to calcultate the Piercing Index

- Answer simple questions labelled A_1 to A_8
- If the vulnerability is X-tenant, only 4 questions must be answered: A1, A2, A7, A8. Otherwise, 6 questions must be answered: A3, A4, A5, A6, A7, A8.

$$\pi = 10 * \frac{\sum log(A_i)}{Max}$$

Max is the maximum possible score obtained by answering the questions.

Max=log(20*1.1*1.21*1.1*1.1*1.1) ≈ 1.55

Section 1: X-tenant boundary violation

Is another customer's data plane accessible within the vulnerable service boundary?

Yes	$\Rightarrow A_1 = 20$
No	$\Rightarrow A_1 = 1$

Is another customer's control plane accessible within the vulnerable service boundary?

Yes	$\Rightarrow A_1 = A_1 * 1.1$
No	$\Rightarrow A_1 = A_1 * 1$

Is the data or control plane of another service accessible within the vulnerable service boundary?

Yes, either the data OR the control plane	$\Rightarrow A_2 = 1.1$
Yes, both data AND control planes	$\Rightarrow A_2 = 1.1 * 1.1 = 1.21$
No, the vulnerability is not X-service	$\Rightarrow A_2 = 1$

Section II: Same-tenant vulnerability

Is this same-tenant vulnerability a X-service boundary violation?

- No, but it permits X-plane boundary violation (data / control planes) $\Rightarrow A_3 = 1.05$
- No, and it does not permit a X-plane boundary violation $\Rightarrow A_3 = 1$
- Yes , it is X-service boundary violation $\Rightarrow A_3 = 1.1$

Does the vulnerability allow illegitimate read access?

- Yes, to the control or data plane of another service $\Rightarrow A_4 = 1.05$
- Yes, to the control or data plane of this service only $\Rightarrow A_4 = 1.05$
- No $\Rightarrow A_4 = 1$

Does the vulnerability allow illegitimate write access?

- Yes, to the control or data plane of another service $\Rightarrow A_5 = 1.05$
- Yes, to the control or data plane of this service only $\Rightarrow A_5 = 1.05$
- No $\Rightarrow A_5 = 1$

What is the maximum scope elevation granted by this vulnerability?

- Whole tenant/organization $\Rightarrow A_6 = 8$
- Subscription/account $\Rightarrow A_6 = 6$
- Resource group $\Rightarrow A_6 = 3$

Section III: Additional information

What is the level of disclosure?

Fully disclosed	$\Rightarrow A_7 = 1.1$
Partially disclosed – key elements removed	$\Rightarrow A_7 = 1$
Undisclosed	$\Rightarrow A_7 = 0.9$

Does it require some insider help to trigger?

Yes, data exfiltration (e.g.: a random ID)	$\Rightarrow A_8 = 0.7$
Yes, user intervention (e.g.: phishing)	$\Rightarrow A_8 = 0.9$
No, but bruteforceable (e.g.: a repo name)	$\Rightarrow A_8 = 1.0$
No	$\Rightarrow A_8 = 1.1$

Example

Let's suppose an AWS X-tenant vulnerability impacts read access to the data plane of one Cloud service. ($A_1 = 20, A_2 = 1.1$).

The exploit has not been disclosed ($A_7 = 0.9$).

User intervention is not required and no extra secret is necessary ($A_8 = 1.1$).

$$\pi = 10 * \frac{\log(20 * 1.1 * 0.9 * 1.1)}{MAX} = 8.6$$

In this example, the piercing index is 8.6. It falls into the red category (ranging between 7.5 and 9.5).