


Jonathan Villarreal	2021-08-31 17:39	comment	Public
<p>@flyingtoasters said..."So, as we dig into this report we are looking to identify if there is a security vulnerability that occurs here (security bug) or if this is just a case of identifying files that are being stored/served which should not be because they may appear to contain personal information (privacy bug)."</p> <p>so @entropython we went from "privacy bug" to "privacy issue"</p> <p>I'm just wondering when Verizon is going to start taking data leaks seriously?</p> <p>This is from the 2021 Verizon Data Breach Report....</p> <p>"A related result that will likely not be surprising is that this year, external cloud assets were more common than on premises assets in both incidents and breaches. Now before you put that in your marketing brochure for your next gen AI21 cloud security product, there were 10 times as many Unknowns (quite plainly incidents where the information on the location of the assets was not available) as there were cloud assets. That is more than enough to tip the scales in the other direction if weâ€™d known more about what happened. Still, in a sample of random organizations, 17% that had a web presence had internet-facing cloud assets.22 If it was not obvious by now, cloud assets deserve a seat at the grown-up security table and a piece of your budget pie."</p> <p>VERIZON HAS CONFIRMED the DATA LEAK. You're own staff called it a "privacy bug"</p> <p>AND YOU REFUSE TO AWARD ME A CRITICAL BOUNTY???</p> <p>VERIZON CONTRACTORS TAX ID, PII &amp; SIGNATURES are 100% LEAKING LIVE RIGHT NOW!!!!</p> <p>You demoted the severity 2 times!!! THIS IS NOT A MEDIUM VULNERABILITY!!!</p> <p>WAKE UP!!!! THE DATA IS LEAKING LIVE RIGHT NOW!!!!</p> <p>IT HAS BEEN LEAKING FOR OVER A MONTH WHEN I REPORTED IT!!!</p> <p>THIS IS LITERALLY THE WORST THING THAT CAN HAPPEN TO A COMPANY!!!!</p> <p>ANYONE CAN ACCESS THIS AT ANY TIME!!!</p>			
Jonathan Villarreal	2021-08-31 21:52	comment	Public
<p>Our program policy lists CWE-389 as Informative {F1433137}, which will not receive a bounty. After an in depth review of the system, files, and customer's account and configuration we have notified the customer of their incorrect usage of the █████ system and it is up to them to take action (remove the files) or not.</p> <p>Whether you want to call it a privacy bug, issue or violation is inconsequential. The system in question █████ is not at fault for exposing the files that you identified. Individual users (customers) of that service uploaded files to be stored and shared through that system. The system's job is to store files when given them, and serve them up when requested █████ is not intended to host potentially private information such as █████ forms, but that does not mean that using it this way is a security issue.</p> <p>Posting about this bug on twitter is in violation of our program policy and may also be against the HackerOne platform Terms</p> <p><a href="#">Screen_Shot_2021-09-01_at_12.16.53_PM.png</a></p> 			
	2021-09-01 16:23	comment	Public
<p>@flyingtoasters</p> <p><b>I'm not brand new, so please don't insult me by telling me that server misconfigurations or lack there of are not at fault for Verizon's data leak.</b></p> <ol style="list-style-type: none"> <li>1. All of the endpoints I called out are running AWS.</li> <li>2. By you saying that the server is not intended to store private information is the exact reason why I'm calling you out on CWE-922 (Insecure Storage of Sensitive Information) NOT your stated CWE-389 "Informative" (Privacy Violation)</li> <li>3. It's clear that the cloud engineers have not hardened the servers because something such as implementing Dataguise (PKWARE) on the servers could have helped prevent this. It is Verizon's job to anticipate and prepare for instances like this, and not try to pass this off as NBD.</li> </ol> <p><b>Here is a resource to help you with mitigation</b></p> <p><a href="https://aws.amazon.com/marketplace/seller-profile?id=7f34d017-3bb3-4efe-bff6-8dc26c137141">https://aws.amazon.com/marketplace/seller-profile?id=7f34d017-3bb3-4efe-bff6-8dc26c137141</a></p> <p>██████ is not intended to host potentially private information such as W9 forms, but that does not mean that using it this way is a security issue."</p> <p>When Verizon failed to implement a server side solution to scan for sensitive data and trusted the product owner not to upload sensitive data, Verizon created a security issue. We are human, we forget, we are not perfect, so software helps us stay compliant. Verizon has consequentially shifted the blame of this data leak onto the product owner and refuses to acknowledge the vulnerability that persists on Verizon's Servers.</p> <p><b>How do you plan on explaining this confirmed data leak to the affected parties?</b></p> <ul style="list-style-type: none"> <li>• The servers were never intended to hold sensitive data?</li> <li>• Its the product owners fault and we have told them to remove the data?</li> <li>• We plan on writing more strict product owner policy?</li> </ul> <p><b>Is marking this Data Leak as informational Verizon's way of sliding past their duty to publicly disclose?</b></p> <ul style="list-style-type: none"> <li>• Yes, posting the TRUTH publicly on Twitter is what I am going to continue to do because this is OUR data that is being compromised. With your acknowledged response, it is evident that Verizon has NO intention of fixing the root cause of the issue - which concerns me even more.</li> <li>• If you do make any server side configurations, that too posses a problem for Verizon as you have stolen from me, and Hackerone.</li> </ul> <p><b>I'm not after a bounty at this point, I want justice, I want honesty and integrity from Verizon &amp; Hackerone</b></p> <p>I'll be posting this online shortly and sending this to the SEC as well. All of your servers need to be audited for knowingly allowing DATA LEAKS that affect peoples lives and can contribute to FRAUD.</p>			
Jonathan Villarreal	2021-09-01 17:35	comment	Public