


As we kick off the new year, it is important to take a look back and understand the major threats of the last year. To do this, we are going to focus on the Zero-Day attacks from the year. While the list of these types of attacks is an extremely large list, Lets dig into a few. For a full list of disclosed Zero-Days, check out the [Zero Day Initiatives](#) website.

Diving into Apple, the company released fixes for [20 Zero-Day attacks](#) this last year. Breaking this down, it equates to about one Zero-Day every two weeks or so. While this is concerning in itself, the discovery of one of the most [sophisticated attacks in Cyber](#) security was also discovered. The attack vector chained multiple Zero-Days include attacks against the underlying hardware. Also, the attack is not only a zero-day but also a zero-click which means that there is no user action needed in order for the attack to take place. The biggest take away from this, in my opinion, is that no system is fully safe. The idea that just because you use an Apple device, you are safe is not the case. While many times they are able to release a patch, the second article highlights that in order to do this, they have to know about the weakness.

Switching gears to Microsoft, the company is celebrating its [20<sup>th</sup> anniversary for Patch Tuesday](#). Taking a look at the last year, the company came in slightly higher than Apple with 23 Zero-Day patches released. While a total of 909 CVEs where addressed throughout the year, this again shows that the Zero-day exploits happen with a frequency of about one every other week. Over half of the exploits discovered involved escalation of privileges with only a small number of them meant for DoS, Remote code execution or information disclosure. The remainder focused on security feature bypass. Having an idea of what attackers are focusing on can help guide the efforts and make business continuity plans where applicable.

[Switching gears](#), let's focus on the top 10 vulnerabilities of the year. While patching systems can generally keep you protected and are of course the best steps to take in most situations, the two most detrimental Zero-Days found in 2023 resulted in a full hardware replacement in order to become fully protected. The discovery of the Barracuda ESG requires devices that have been infected to be immediately replaced.



The second take away on the top ten list is not only to patch systems in production but to also ensure that any backups receive the backups as well. This is shown from the MoveIT transfer attack that continues to see the attack having success months after the release of the corrective patch.

As we move into the start of the year, it is important that we remember to keep up with our entire inventory of not only hardware but also any software that is in use to ensure that the security posture can remain as high as possible.

"If you cannot afford security, you cannot afford a breach" -phr00ts

Thank you,

Caleb Leggett

