Zero Day Attack

Describes newly discovered security vulnerabilities that hackers use to attack a system. It refers to the fact that the vendor or developer has just learned of a flaw, meaning they have had “zero days” to fix it. It is very important to understand the difference between vulnerability, exploit, attack.

- Vulnerability: It is the gateway that a cybercriminal uses to affect a specific system, since the developers are not aware of its existence and there are no security patches.
- Exploit: It is the attack method that cybercriminals use to attack a system with the unpatched vulnerability.
- Attack: It is the use of the zero-day exploit to cause damage or steal data from an infected system.

Examples

Chrome Vulnerability

In 2021, Google Chrome suffered a series of threats of this style, which caused Chrome to release updates for this vulnerability, which was due to an error in the V8 JavaScript search engine used by this browser.

Apple iOS

In 2020, it fell victim to at least two sets of iOS zero-day vulnerabilities, including a zero-day bug that allowed attackers to remotely compromise iPhones.

Zoom

In 2020, a vulnerability was found in this platform; which allowed cybercriminals to remotely access the computer of a user using an older version of Windows.