## Zero-Day Vulnerabilities

A zero-day vulnerability is a vulnerability or bug that is unknown to trusted sources, such as operating system and antivirus vendors. Operating system vendors write and release patches once they know about them, but the vulnerability remains until the vendors know about them.

As an example, the Heartbleed vulnerability existed for a couple of years before it was widely published. Up until the time that OpenSSL developers released a fix, everyone using it was vulnerable.

Users might adopt the idea that up-to-date antivirus software will protect them from all malware. This simply isn’t true. No matter how great an antivirus company is at identifying new malware, there will always be a lag between the time when criminals release the malware, and the antivirus company releases new signatures to discover it. This is especially true when attackers are releasing more than 200,000 new variants of malware daily. This includes malware designed to take advantage of zero-day vulnerabilities.

Zero-day exploits take advantage of vulnerabilities that don’t have available patches. It could be because vendors don’t know about the vulnerability or haven’t written patches to fix it yet. Zero-day exploits can evade up-to-date antivirus software.

Mitigation :

Log4j

Resouces :

1. CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide - Darril Gibson