Case Study 1: Operating System Security

Windows WannaCry Ransomware (2017)

Nature of the Vulnerability: A ransomware attack exploiting the EternalBlue vulnerability in Windows SMB protocol.
How it was Exploited: It spread rapidly across networks by exploiting unpatched Windows systems, encrypting files and demanding ransom in Bitcoin.
Patches/Solutions Provided: Microsoft released emergency patches for supported and even unsupported versions of Windows.
Lessons Learned: Regular system updates, timely patching, and network segmentation are critical to prevent widespread attacks.

Linux Dirty COW (2016)

Nature of the Vulnerability: A privilege escalation vulnerability in the Linux kernel's memory subsystem.
How it was Exploited: Attackers could exploit a race condition to gain root access on vulnerable systems.
Patches/Solutions Provided: Linux distributions quickly released kernel patches to fix the vulnerability.
Lessons Learned: Kernel-level flaws can exist for years unnoticed, highlighting the need for continuous code review and fast patch application.

macOS Gatekeeper Bypass (2019)

Nature of the Vulnerability: A flaw in Apple's Gatekeeper allowed unverified apps to run without proper security checks.
How it was Exploited: Attackers could trick users into downloading malicious apps that bypassed Gatekeeper restrictions.
Patches/Solutions Provided: Apple issued a security update to strengthen Gatekeeper validation.
Lessons Learned: Relying solely on built-in protections is risky; users must remain cautious when downloading applications.

Android Stagefright Vulnerability (2015)

Nature of the Vulnerability: A critical flaw in the Android media playback engine 'Stagefright.'
How it was Exploited: Attackers sent malicious MMS messages that could execute code without user interaction.
Patches/Solutions Provided: Google and device manufacturers released security patches, though fragmentation delayed widespread fixes.
Lessons Learned: Mobile OS fragmentation makes timely updates difficult; consistent patch delivery is essential.

Solaris Telnet Vulnerability (2010)

Nature of the Vulnerability: A default configuration flaw in Solaris telnet service allowed unauthorized remote access.
How it was Exploited: Attackers could log in remotely without authentication using a simple exploit.
Patches/Solutions Provided: Oracle released patches and advised administrators to disable the telnet service in favor of SSH.
Lessons Learned: Default insecure services should always be disabled; administrators must prioritize secure configurations.