OWASP #8 – Software and Data Integrity Failures

Gavin Lillard (IST-103)

As stated on SecurityJourney.com (2023), this vulnerability allows potential attackers to modify or delete data in an unauthorized manner. Said vulnerability allows exploits that extract sensitive data and damages the system. Examples provided by SecurityJourney.com (2023) include insufficient verification of data authority, missing support for integrity checks, untrusted search path, download of code without integrity checks, and deserialization of untrusted data. I will put into my own words what those examples mean. Starting with insufficient verification of data authority, a premature verification allowing a potential attacker to inject their own data into the system. Missing support for integrity checks, insufficient verification software allowing potential attackers to manipulate data undetected. Untrusted search path, when potential attackers change the search path for used libraries/modules allowing them to inject their own data into the system. Download of code without integrity, this is a premature verification for a download allowing a potential attacker to inject their own code. Finally, deserialization of untrusted data, again a premature verification opening a window for potential injection of attacker code.

SecurityJournery.com (2023) suggests that the implementation of security updates/patches swiftly, compilation of a SBOM and regular monitoring system updates/patches for security will ensure mitigation against software and integrity failures. It is crucial to be attentive to your software throughout your application’s life.

Works Cited

Anon. “OWASP Top 10 Software and Integrity Failures Explained.” *Www.securityjourney.com*, 14 Sept. 2023, www.securityjourney.com/post/owasp-top-10-software-and-integrity-failures-explained.