LOGJAM SSL Vulnerability

The Logjam vulnerability is a security flaw in the TLS protocol that allows attackers to weaken the encryption of HTTPS connections by forcing them to use weak, export-grade cryptography. It specifically targets the Diffie-Hellman key exchange process, exploiting its use of common prime numbers. This vulnerability makes it feasible for attackers to intercept and decrypt communications, posing a significant threat to data confidentiality.

How to fix the Logjam vulnerability ?

1. **Disable Export-Grade Cipher Suites**: Update your server configuration to disable all export-grade cipher suites, particularly those using DHE_EXPORT, which are vulnerable to the Logjam attack.
2. **Use Strong Diffie-Hellman Groups**: Replace the Diffie-Hellman parameters with a strong, unique prime of at least 2048 bits. Avoid using common or weak DH parameters.
3. **Enforce TLS 1.2 or Higher**: Configure your servers to use TLS 1.2 or higher, as these versions offer more robust security features and are not susceptible to the same downgrade attacks

---

Revision #1
Created 9 November 2023 06:27:16 by Admin
Updated 9 November 2023 06:38:58 by Admin