SQL Server patches and their types:

Patch Type	Description	Frequency	Components Updated	Application
Service Packs (SP)	Major cumulative updates that include new features, improvements, and all previous patches.	Typically every 12-18 months (Discontinued after SQL Server 2016).	SQL Server Engine, Reporting Services, Integration Services, etc.	Manual installation, often planned.
Cumulative Updates (CU)	Includes all fixes since the last service pack or previous CU, adding minor feature improvements and security fixes.	Every month for the first year, quarterly after that.	Bug fixes, performance enhancements, and security patches.	Manual or automated installation.
General Distribution Releases (GDR)	Patches released for critical security vulnerabilities. Only includes essential security fixes, not new features or other fixes.	As needed (ad-hoc).	Critical security patches.	Mandatory, especially for security.
Hotfixes (QFE)	Targeted patches released to fix specific critical issues impacting SQL Server functionality.	As needed (ad-hoc, rare).	Very specific bug or issue affecting the server.	Should be applied only when necessary.
Security Updates	Security-specific updates addressing vulnerabilities in SQL Server.	Typically monthly (part of Microsoft Patch Tuesday).	Critical security fixes and patches.	Mandatory for security compliance.
On-Demand Hotfixes	Address high-priority issues reported by customers. Released on-demand by Microsoft.	As needed (rare).	Fixes critical, unplanned issues that require immediate attention.	Should be evaluated before application.

Best Practices for Applying SQL Server Patches:

1. **Test in Development**: Always test patches in a non-production environment before applying them to the production server.
2. **Backup Before Patching**: Ensure backups of databases and system configurations are taken before applying patches.
3. **Stay Current on Cumulative Updates**: CUs provide important bug fixes and enhancements.
4. **Monitor Security Bulletins**: Keep track of security updates and GDR releases to address vulnerabilities promptly.
5. **Plan for Downtime**: Some patches may require server restarts, so plan downtime accordingly.
6. **Automate Patch Management**: Use tools like **Microsoft Update** or third-party patch management software to automate the installation of patches.

Patching your SQL Server regularly helps ensure performance, security, and stability.