Code Injection: What it is, how it leads to RCE, and how to prevent it

Gridinsoft Help Center

What it is

How it works

- A vulnerable app trusts input (form fields, uploads, API calls).
- The attacker crafts input that breaks out of normal handling.
- Their code executes-downloading payloads, stealing data, or taking control.

What you might notice

- Sudden processes you didn’t start; new services or tasks
- Unusual outbound connections right after a form submit/upload
- AV/EDR alerts about script hosts, PowerShell, or injected DLLs

If you suspect it

- Isolate the host; preserve logs and memory.
- Block the offending URL/IP at WAF/firewall.
- Patch/disable the vulnerable feature; rotate secrets/keys.
- Hunt laterally for dropped payloads and persistence.

Prevent it

- Validate and sanitize all inputs; treat uploads as untrusted.
- Use allow-lists (what’s allowed) rather than block-lists.
- Turn on WAF/Runtime protections (e.g., RASP) and strict content security.
- Keep apps, libraries, and frameworks updated; avoid risky plugins.
- Run services with least privilege; restrict script interpreters.