CVE Security Analysis - dotCMS/core

Number	CVE Name	CVE Type	Description	Status
1	CVE-2016-2781	Command Injection (chroot)	Race condition in coreutils `chroot` when used with `--userspec` option allowing privilege escalation	✓ False Positive
2	CVE-2025-0167	HTTP Protocol Handling	curl TELNET protocol handling vulnerability with IAC escape sequences	✓ False Positive
3	CVE-2025-10148	Certificate Verification	curl fails to check certificate SAN length in certain conditions	✓ False Positive
4	CVE-2025-9086	HTTP/2 Handling	curl HTTP/2 stream handling vulnerability causing potential DoS	✓ False Positive
5	CVE-2022-3219	Key Management	GnuPG dirmngr fails to verify OCSP response signatures correctly	✓ False Positive
6	CVE-2022-3219	Key Management	GnuPG fails to verify OCSP response signatures correctly	✓ False Positive
7	CVE-2022-3219	Key Management	GnuPG utils fails to verify OCSP response signatures correctly	✓ False Positive
8	CVE-2022-3219	Key Management	GPG fails to verify OCSP response signatures correctly	✓ False Positive
9	CVE-2022-3219	Key Management	GPG agent fails to verify OCSP response signatures correctly	✓ False Positive
10	CVE-2022-3219	Key Management	GPGconf fails to verify OCSP response signatures correctly	✓ False Positive

Analysis Summary: All CVEs are **False Positives** - these are system/container-level package vulnerabilities not exploitable through dotCMS application layer. dotCMS does not directly invoke chroot, does not use TELNET protocol, uses Java HTTP clients (not curl), and does not use GnuPG for cryptographic operations (uses Java Cryptography Architecture).