dotCMS Security Analysis: CVE Assessment

#	CVE ID	CVE Type	Description	Status
1	CVE-2016-2781	Command Injection in coreutils (chroot)	Vulnerability in GNU coreutils chroot command allowing privilege escalation through TIOCSTI ioctl. Impact limited to systems where chroot is directly invoked without supplementary security.	✕ **False Positive** - dotCMS does not invoke chroot command directly; runs in containerized/JVM environments with standard user privileges; no evidence of coreutils command execution in core codebase
2	CVE-2025-0167	HTTP Request Smuggling in curl	curl vulnerability related to HTTP/2 pseudo-headers handling that could lead to request smuggling attacks when curl acts as intermediary.	✕ **False Positive** - dotCMS uses Java-based HTTP clients (Apache HttpClient, HttpURLConnection); curl is container dependency, not used programmatically; internal HTTP handling uses Java HTTP stack
3	CVE-2025-10148	Information Disclosure in curl	curl vulnerability exposing sensitive information through improper handling of redirects or authentication tokens.	✕ **False Positive** - Same rationale as CVE-2025-0167; dotCMS application layer does not invoke curl binary; Java HTTP clients handle all HTTP operations with built-in security controls
4	CVE-2025-9086	Denial of Service in curl	curl vulnerability allowing DoS through malformed input or resource exhaustion in specific protocol handlers.	✕ **False Positive** - Same rationale as CVE-2025-0167; curl is OS-level package not utilized by dotCMS application; Java-based HTTP handling with timeout configurations and resource management
5	CVE-2022-3219	Denial of Service in GnuPG (dirmngr component)	GnuPG dirmngr component vulnerable to DoS through certificate verification process. Affects dirmngr, gnupg-utils, gpg, gpg-agent, gpgconf packages.	✕ **False Positive** - dotCMS does not use GnuPG for cryptographic operations; uses Java Cryptography Architecture (JCA) and Bouncy Castle; GnuPG packages are base OS dependencies not invoked by application; PGP/GPG functionality not present in core features

Summary

All CVEs: False Positives ✓

All identified vulnerabilities affect OS-level packages (coreutils, curl, gnupg) that are container/system dependencies but are not utilized by the dotCMS Java application layer. dotCMS implements its own security controls using Java-native libraries and frameworks, effectively isolating the application from these system-level vulnerabilities.