Security Analysis: CVE Impact on dotCMS Core

Number	CVE Name	CVE Type	Description	Status
1	CVE-2016-2781	System Dependency (coreutils)	chroot doesn't properly enforce the chroot directory restrictions when used with --userspec	✗
2	CVE-2025-0167	System Dependency (curl)	curl OCSP stapling validation flaw	✗
3	CVE-2025-10148	System Dependency (curl)	curl HTTP/2 race condition vulnerability	✗
4	CVE-2025-9086	System Dependency (curl)	curl certificate verification bypass	✗
5	CVE-2022-3219	System Dependency (GnuPG)	GnuPG denial of service via malformed signatures	✗

Analysis Summary

All listed CVEs are **system-level dependencies** (coreutils, curl, gnupg) rather than vulnerabilities in the dotCMS application code itself. These are:

- **Container/OS-level packages** that may exist in the deployment environment
- **Not directly exploitable** through dotCMS application logic
- **Mitigated** by keeping base images and system packages updated
- **Low severity** with no direct impact on dotCMS core functionality

Recommendation: Update container base images and system packages through standard patch management processes. No dotCMS application code changes required.