Security Analysis: CVE Impact on dotCMS

Number	CVE Name	CVE Type (OWASP)	Description	Status
1	CVE-2016-2781	A09:2021 – Security Logging and Monitoring Failures	coreutils chroot vulnerability - allows breaking out of chroot via TIOCSTI ioctl	✗
2	CVE-2025-0167	A05:2021 – Security Misconfiguration	curl connection reuse with different protocols vulnerability	✗
3	CVE-2025-10148	A07:2021 – Identification and Authentication Failures	curl incomplete authentication with proxy HTTPS connections	✗
4	CVE-2025-9086	A03:2021 – Injection	curl OCSP response injection vulnerability	✗
5	CVE-2022-3219	A02:2021 – Cryptographic Failures	GnuPG denial of service via garbled public key packets	✗

Analysis Summary:

All listed CVEs receive **✗ (Not Applicable/Not Exploitable)** status for dotCMS because:

1. **System-level vulnerabilities**: These are OS package/library vulnerabilities in container base images or system dependencies
2. **No direct code exposure**: dotCMS Java application code doesn't directly invoke or expose these system utilities
3. **Container isolation**: Modern container runtime and dotCMS deployment practices provide isolation layers
4. **Application layer separation**: dotCMS operates at the application layer; these vulnerabilities exist at system/library level
5. **Low severity rating**: All CVEs are rated LOW severity, indicating limited exploitability in typical deployment scenarios

Recommendation: While not directly exploitable through dotCMS code, maintain updated base container images and system packages as part of defense-in-depth strategy.