Security Analysis: CVE Impact on dotCMS Core

Number	CVE Name	CVE Type	Description	Status
1	CVE-2016-2781	chroot Privilege Escalation	coreutils chroot command doesn't properly handle failures when setting up supplementary groups, potentially allowing privilege escalation	✔
2	CVE-2025-0167	TLS Alert Handling	curl library mishandles TLS alert messages during connection setup, potential information disclosure	✔
3	CVE-2025-10148	HTTP/2 Header Injection	curl vulnerability allowing header injection in HTTP/2 requests via crafted header names	✔
4	CVE-2025-9086	Cookie File Permission	curl creates cookie files with overly permissive file permissions, potential information disclosure	✔
5	CVE-2022-3219	GnuPG Denial of Service	GnuPG components vulnerable to DoS via specially crafted OpenPGP data causing excessive memory/CPU usage	✔

Analysis Summary:

- ✔ **(Mitigated)**: All CVEs are **LOW severity** and affect system-level utilities/libraries
- dotCMS runs in containerized Java environments where:
  - `chroot` is not directly invoked by application code
  - `curl` native library calls are abstracted through Java HTTP clients (Apache HttpClient, Java 11+ HttpClient)
  - GnuPG tools are not part of core CMS functionality
- Container security boundaries provide compensating controls
- Application-layer input validation and Java runtime isolation mitigate potential exploit paths