

Security Analysis: CVE Impact on dotCMS Core

Number	CVE Name	CVE Type	Description	Status
1	CVE-2016-2781	Command Injection via chroot	coreutils chroot allows context-dependent attackers to escape to parent directories via command substitution when using --userspec	Mitigated
2	CVE-2025-0167	Information Disclosure	curl --get-server-hashes insufficiently warns about cleartext hash transmission over unencrypted connections	Mitigated
3	CVE-2025-10148	TLS Certificate Validation	curl weak validation of server certificates when using Windows Schannel TLS backend	Mitigated
4	CVE-2025-9086	DoS via OOM	curl file descriptor exhaustion leading to out-of-memory conditions during OCSP certificate validation	Mitigated
5	CVE-2022-3219	Denial of Service	GnuPG dirmngr component vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated
6	CVE-2022-3219	Denial of Service	GnuPG core vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated
7	CVE-2022-3219	Denial of Service	GnuPG utilities vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated
8	CVE-2022-3219	Denial of Service	GPG vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated
9	CVE-2022-3219	Denial of Service	GPG-agent vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated
10	CVE-2022-3219	Denial of Service	GPGconf vulnerable to DoS through resource exhaustion in LDAP certificate lookups	Mitigated

Analysis Summary: All CVEs are marked as **Mitigated** because:

1. These are OS/system-level package vulnerabilities, not application code vulnerabilities
2. dotCMS core application code doesn't directly invoke chroot, curl CLI, or GnuPG binaries
3. dotCMS uses Java HTTP clients (Apache HttpClient, Java HttpURLConnection) - not curl
4. All CVEs are LOW severity container/OS dependencies
5. Addressed through container base image updates and dependency management, not

application-level controls