

Issues » Incorrect access control can lead to information disclosure and remote execution

Issue:	SI-54
Date:	Jan 9, 2020, 10:30:00 AM
Severity:	Critical
Requires Admin Access:	No
Fix Version:	5.2.4
Credit:	Internal Security Team
Description:	<p>dotCMS fails to normalize the URI string when checking if a user should have access to a specific directory. If a dotCMS installation stores its assets under the tomcat's webapps/ROOT/assets directory, then the files and data stored under this directory can be accessed by crafting a uri that traverses the directory structure, like so:</p> <p>http://localhost:8080/234aa/test/../../assets/messages/cms_language_en.properties</p> <p>Additionally, when files are uploaded into dotCMS, it creates a temporary file which lives under the /assets directory and whose location is knowable. This allows a malicious user to upload an executable file such as a jsp and use it perform remote command execution with the permissions of the user running the dotCMS application.</p>
Mitigation:	<p>If you are unable to upgrade to dotCMS 5.2.4 or higher, there are workarounds that can be applied:</p> <ol style="list-style-type: none">1. The dotCMS /assets and /dotsecure should be stored in a folders outside of the webapps/ROOT directory. You can configure your dotCMS to load these from external locations in the dotmarketing-config.properties file by setting these variables: <pre>ASSET_REAL_PATH=/data/shared/assets DYNAMIC_CONTENT_PATH=/data/local</pre> <ol style="list-style-type: none">2. OSGI plugin fix: dotCMS has created an OSGI plugin that normalizes any URI passed to dotCMS which mitigates the issue. This plugin can be found here: https://github.com/dotCMS/com.dotcms.filter.urinormalizer. This plugin can be dynamically loaded into a 5 series dotCMS instance and will mitigate the issue.3. Add constraint to web.xml: Additionally, if you are unable to move your /assets directory, you can add constraints to your web.xml to prevent unauthorized access to your ./assets and ./dotsecure directories, as detailed in this issue: https://github.com/dotCMS/core/issues/17835
References	<p>CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6754</p> <p>GitHub: https://github.com/dotCMS/core/issues/17796</p>

dotCMS is designed to deliver content driven applications at scale. Whether you're building a network of global websites, an employee intranet, customer portal, or single page web application, dotCMS helps you manage content, images, and assets in one centralized location and deliver them to any channel.

PRODUCT	SOLUTIONS	COMPANY
dotCMS Cloud	Content Management	Events
Pricing	Headless/APIs	Careers
14 Day Trial	Asset Management	News Room
Feature List	Agile E-Commerce	Contact Us
	Intranets & Extranets	

