Issues » Matrix URI parameters can expose private assets

Issue:	SI-63
Date:	Jun 14, 2022, 1:45:00 PM
Severity:	Moderate
Requires Admin Access:	No
Fix Version:	22.06, 22.03.2, 21.06.9, 5.3.8.12
Credit:	Fortinet (https://www.fortinet.com/)
Description:	Some Java Application frameworks, including those used by Spring or Tomcat, allow the use of "matrix parameters" — URI parameters separated by semicolons. Through precise semicolon placement in a URI, it is possible to exploit this feature to avoid dotCMS's path-based XSS prevention/require login filters and access restricted resources. For example, the semicolon in the URL below would reveal to anyone a text file ordinarily only visible to signed-in users: `https://demo.dotcms.com/html;/js/dojo/README-Building-dojo-for-dotCMS.txt` The ability to circumvent these filters can be chained with other code to expolit dotCMS using XSS attacks.

Mitigation:	## Upgrade
	dotCMS recommends upgrading to one of the versions of dotCMS patched against this vulnerability, which include the following, as well as subsequent versions:
	- **Agile:**
	  - 22.06+
	- **LTS:**
	  - 22.03.2+
	  - 21.06.9+
	  - 5.3.8.12+
	
	## WAF Rule
	It is possible to create a WAF rule that disallows **;** (semi-colons) specifically in the the URI portion of a request URL. This would effectivily block any exploit of the vunerability.
	
	## Hotfix Plugin
	dotCMS 5.1.6+
	The following OSGi plugin, designed to work with versions dotCMS 5.1.6 and later, can be used to mitigate the issue in running dotCMS instances:
	- https://github.com/dotCMS/patches-hotfixes/tree/master/com.dotcms.security.matrixparams
	
	## dotCMS Cloud
	dotCMS has already applied mitigations for this issue to all dotCMS Cloud customers; no action is needed.

References	- GitHub Issue Link - MatrixParameter Security Interceptor hotfix plugin - CVE Reference CVE-2022-35740