

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:	<p>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.</p> <p>For example, the semicolon in the URL below would reveal to anyone a text file ordinarily only visible to signed-in users:</p> <p><code>https://demo.dotcms.com/html;/js/dojo/README-Building-dojo-for-dotCMS.txt</code></p> <p>The ability to circumvent these filters can be chained with other code to exploit dotCMS using XSS attacks.</p>



Mitigation:	<h2>Upgrade</h2> <p>dotCMS recommends upgrading to one of the versions of dotCMS patched against this vulnerability, which include the following, as well as subsequent versions:</p> <ul style="list-style-type: none"> • Agile: <ul style="list-style-type: none"> ◦ 22.06+ • LTS: <ul style="list-style-type: none"> ◦ 22.03.2+ ◦ 21.06.9+ ◦ 5.3.8.12+ <h2>WAF Rule</h2> <p>It is possible to create a WAF rule that disallows ; (semi-colons) specifically in the the URI portion of a request URL. This would effectively block any exploit of the vulnerability.</p> <h2>Hotfix Plugin</h2> <p>dotCMS 5.1.6+</p> <p>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:</p> <ul style="list-style-type: none"> • https://github.com/dotCMS/patches-hotfixes/tree/master/com.dotcms.security.matrixparams <h2>dotCMS Cloud</h2> <p>dotCMS has already applied mitigations for this issue to all dotCMS Cloud customers; no action is needed.</p>
References	<ul style="list-style-type: none"> • GitHub Issue Link • MatrixParameter Security Interceptor hotfix plugin • CVE Reference CVE-2022-35740

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

dotCMS Cloud
Pricing
14 Day Trial
Feature List

SOLUTIONS

Content Management
Headless/APIs
Asset Management
Agile E-Commerce
Intranets & Extranets

COMPANY

Events
Careers
News Room
Contact Us





Copyright © 2011-2022 dotCMS, LLC All rights reserved.

[Privacy](#) | [GDPR Support](#) | [Cookie Settings](#)

