Talos Vulnerability Report

TALOS-2022-1539

WWBN AVideo image403 cross-site scripting (XSS) vulnerability

AUGUST 16, 2022

CVE NUMBER

CVE-2022-30690

SUMMARY

A cross-site scripting (xss) vulnerability exists in the image403 functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

WWBN AVideo 11.6
WWBN AVideo dev master commit 3f7c0364

PRODUCT URLS

AVideo - https://github.com/WWBN/AVideo

CVSSV3 SCORE

9.6 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CWE

CWE-79 - Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

DETAILS

AVideo is a web application, mostly written in PHP, that can be used to create an audio/video sharing website. It allows users to import videos from various sources, encode and share them in various ways. Users can sign up to the website in order to share videos, while viewers have anonymous access to the publicly-available contents. The platform provides plugins for features like live streaming, skins, YouTube uploads and more.

The PHP file `view/img/image403.php` is used by AVideo to show 403 errors, optionally with a custom error message.

```
header('HTTP/1.0 403 Forbidden');
if (empty($_REQUEST['403ErrorMsg'])) {
    $_REQUEST['403ErrorMsg'] = __("You are not allowed to enter here");
}
$_REQUEST['403ErrorMsg'] = "<h1>{$_REQUEST['403ErrorMsg']}</h1>";
if (class_exists("User") && !User::isLogged()) {
    $_REQUEST['403ErrorMsg'] .= '<h2><a target="_blank" href="' .
$global['webSiteRootURL'] . 'user">' . __("Login") . '</a></h2>';
}
?>
...
echo $_REQUEST['403ErrorMsg'];  // [1]
```

The custom error message is taken by `$_GET` or `$_POST` [1] unsanitized, and displayed in the page, leading to a straightforward reflected cross-site scripting (XSS) issue. This can be used by an attacker, in the worst case, to take over an administrator account, for example by tricking an administrator into clicking on a link that triggers the XSS.

Exploit Proof of Concept

```
curl -k 'https://192.168.1.200/view/img/image403.php?
403ErrorMsg=%3Cscript%3Ealert(document.cookie)%3C/script%3E'
```

VENDOR RESPONSE

Vendor confirms issues fixed on July 7th 2022

TIMELINE

2022-07-05 - Vendor Disclosure

2022-07-07 - Vendor Patch Release

2022-08-16 - Public Release

CREDIT

Discovered by Claudio Bozzato of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2022-1538

NEXT REPORT

TALOS-2022-1540