Missing access controls 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 08:01:39 +0000

Title: Missing access controls

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-2020-28861

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 web application was found to provide several endpoints which allowed for unauthenticated data retrieval in a CSV format.

2. PoC

The following requests will retrieve data associated with the projects. The ProjectsCSV endpoint will retrieve all project information present in the system.

https://example.com/Stream/AlbumCSV

https://example.com/Stream/KeywordsCSV

https://example.com/Stream/ProjectKeywordsCSV

https://example.com/Stream/ProjectsCSV

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/>

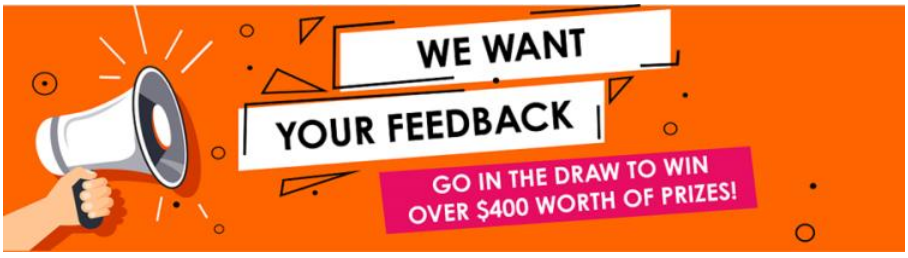
<https://www.facebook.com/The-Missing-Link-268395013346228/?ref=bookmarks>

<https://twitter.com/TML_au>

<https://www.youtube.com/channel/UC2kd4mDmBs3SjW4lX3fFHnQ>

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

<https://forms.office.com/Pages/ResponsePage.aspx?id=XZw2opTdq0iPe7AFmjygSPnqgoolWREpgCEhJxsz3FUMUxTOUREUVRDTzBNQ0pKTkFaS1lETEFaSi4u>



Attachment: smime.p7s
Description:

By Date By Thread

Current thread:

Missing access controls 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
Nmap Announce
Security Tools
Vuln scanners
About
About/Contact