

Site Search

<u>Full Disclosure</u> mailing list archives





List Archive Search



Missing access controls in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure

From: Jack Misiura via Fulldisclosure <full disclosure () seclists org> $\it Date$: 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

ā

9-11 Dickson Avenue

Artarmon

NSW

2064

1300 865 865

+61 2 8436 8585

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

- 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/

UREUVRDTzBNQ0pKTkFaS11ETEFaSi4u>

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.







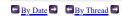
0





Attachment: smime.p7s Description:

Sent through the Full Disclosure mailing list https://nmap.org/mailman/listinfo/fulldisclosu https://nmap.org/maiimai Web Archives & RSS: http



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







Ref Guide Install Guide Docs Download

Nmap OEM

User's Guide
API docs
Download
Npcap OEM

Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Password audit
Web scanners
Wireless
Exploitation

Privacy
Advertising
Nmap Public Source
License



