



# CVE-2020-28856

Published on: 12/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:26 PM UTC

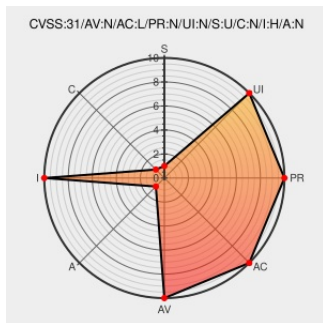
## CVE-2020-28856

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Digital Asset Management](#) from [Openasset](#) contain the following vulnerability:

OpenAsset Digital Asset Management (DAM) through 12.0.19 does not correctly determine the HTTP request's originating IP address, allowing attackers to spoof it using X-Forwarded-For in the header, by supplying localhost address such as 127.0.0.1, effectively bypassing all IP address based access controls.

CVE-2020-28856 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>HIGH</b>	<b>NONE</b>

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Full Disclosure: IP access control bypass in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure	<a href="#">Mailing List</a> <a href="#">Third Party Advisory</a> <a href="#">seclists.org</a>	<a href="#">FULLDISC 20201211 IP access control bypass in OpenAsset Digital Asset Management 11.2.1/12.0.19 disclosure</a>

text/html

Advisory cve-2020-28856

Third Party Advisory

www.themissinglink.com.au

text/html

MISC [www.themissinglink.com.au/security-advisories-cve-2020-28856](http://www.themissinglink.com.au/security-advisories-cve-2020-28856)

OpenAsset | Digital Asset Management Software

Product

openasset.com

text/plain

MISC [openasset.com](http://openasset.com)

OpenAsset Digital Asset Management IP Access Control Bypass ~ Packet Storm

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

MISC [packetstormsecurity.com/files/160453/OpenAsset-Digital-Asset-Management-IP-Access-Control-Bypass.html](http://packetstormsecurity.com/files/160453/OpenAsset-Digital-Asset-Management-IP-Access-Control-Bypass.html)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openasset	Digital Asset Management	All	All	All	All
cpe:2.3:a:openasset:digital_asset_management:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)