

Week 29_ Shodan과 IoT

Refactoring Study

2022.07.30 Kwon Moonjeong

IoT 서비스에서의 보안 취약점

- 사물인터넷 서비스에서 다음과 같은 보안 서비스가 침해될 수 있음
 - IoT 기기 및 서비스 무단 접속: 기기 인증(Entity Authentication) 우회 접근, 초기 설정 비밀번호 정탐
 - 데이터 유출: 기밀성(Confidentiality) 침해
 - 서비스 거부: 가용성(Availability) 침해
- 사물인터넷 기기의 경우 자원(가용 메모리, CPU 연산 능력 등)이 제한적인 특성으로 서비스 거부 공격에 취약함
- 정보 유출을 방지하기 위해 IoT 기기는 서비스에 접근 가능한 사용자를 식별하고 인증할 수 있어야 함
- 무선으로 전송되는 데이터는 도청이나 유출이 용이하므로 암호화해서 기밀성을 제공해야 함
- IoT 서비스 환경에서 특별히 고려할 사항은 장치의 경량 특성임
→ IoT에 많이 적용되고 있는 경량 기기는 자원이 제한적이어서 적용되는 보안 기술도 경량화 필요

IP카메라의 특징

- **IP카메라란?** : “네트워크 카메라”라고도 하며, 카메라 자체에 웹서버 기능을 장착하여 네트워크로 연결되는 카메라. 네트워크 카메라, **Webcam**이라고도 하며, 인터넷 프로토콜 (**IP**)을 사용하여 고속 이더넷 연결을 통해 비디오 및 이미지를 전송
- 기본적으로 제공하는 **DDNS** 주소/**IP**카메라 고유 이름 **OR** 직접 지정하여 **URL** 확보
→ 직접 지정 시, 외부로 연결되는 공인 아이피를 그대로 쓸 수도 있음
- * **DDNS(Dynamic DNS, 동적 DNS)** : 실시간으로 **DNS**를 갱신하는 방식.
유동 **IP**를 고정 **IP**처럼 사용할 수 있도록 해주는 시스템.
컴퓨터에 현재 할당되어 있는 **IP**를 통보받아 **IP**를 **Domain:IP** 쌍으로 기억함.
- 기본적으로 **80번, 8080** 포트로 외부에서 접속 가능

IP카메라의 특징

- CCTV와의 차이점

- CCTV : “폐쇄회로 텔레비전”의 줄임말로, 로컬 저장장치에 영상 정보를 저장하여 일정기간 보관 후 영상이 폐기됨
→ 원격 접근이 제한적이므로 영상 유출의 가능성이 적음
- IP카메라 : 로컬 하드 드라이브에 녹화하는 대신 클라우드에 기록하는 경우가 많으며, 대개 카메라 제조업체의 자체 서버를 활용. 실시간으로 보호자 등의 열람권자에게 영상정보를 네트워크를 통해 전송
→ 네트워크를 통해 영상이 전달되므로 유출의 가능성이 높음

- **Shodan 검색 중 가장 인기가 있는 Webcam** (<https://www.fnnews.com/news/201810100630464173>)
: 국회 과학기술정보방송통신위원회 소속 송희경 자유한국당 의원이 쇼단에서 가장 인기 많은 필터인 웹캠(webcam)으로 검색한 결과 한국은 404개가 검색돼 검색되는 국가들 중 세번째로 많은 것으로 나타났다. 또 'CCTV' 검색 건수는 1140건으로 각 국가들 중 가장 많이 검색된 것으로 확인됐다.

IP카메라의 벤더사별 기본 장치 정보

회사 이름	기본 계정	기본 포트
DAHUA	id : admin / pw : 888888	37777 / 37778
나다텔	id : admin / pw : 123456	5445 ~ 5447
HIKVISION	id : admin / pw : 12345	80 / 8000 / 554
스카이렉스	id : admin / pw : 1234	8602
이지피스	id : admin / pw : 1111 혹은 암호 없음	8000 / 8001
삼성 테크윈	id : admin / pw : 4321	4520~4524 / 8080

Shodan으로 검색하기 (1) IP 카메라

비밀번호 없이 공개된 IP 카메라 중 webcam 7(윈도우용 IP 카메라 서버) 찾기
webcam product:"webcam 7 httpd"


← → ↺ [https://www.shodan.io/search?query=webcam+product%3A\"webcam 7\"](https://www.shodan.io/search?query=webcam+product%3A\) 🔍 📄 ☆ 📧 ⚙️ 📱

Gmail 지도 YouTube 웨이브 (wavve) 취업 선진회계법인 쿠팡플레이 - 와우 회...

SHODAN Explore Downloads Pricing [webcam product:\"webcam 7\"](#) 🔍 Account

TOTAL RESULTS
122

TOP COUNTRIES



Germany	34
United States	16
Spain	10
Serbia	8
Russian Federation	8
More...	

TOP PORTS

8080	66
80	18
9999	7
8081	5
8888	5
More...	

TOP ORGANIZATIONS

Deutsche Telekom AG	26
---------------------	----

View Report Download Results Historical Trend Browse Images View on Map


New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

webcam 7

194.37.1.82
194.37.1.82 eth.pskt.spb.ru
P.A.K.T LLC
 Russian Federation, Saint Petersburg

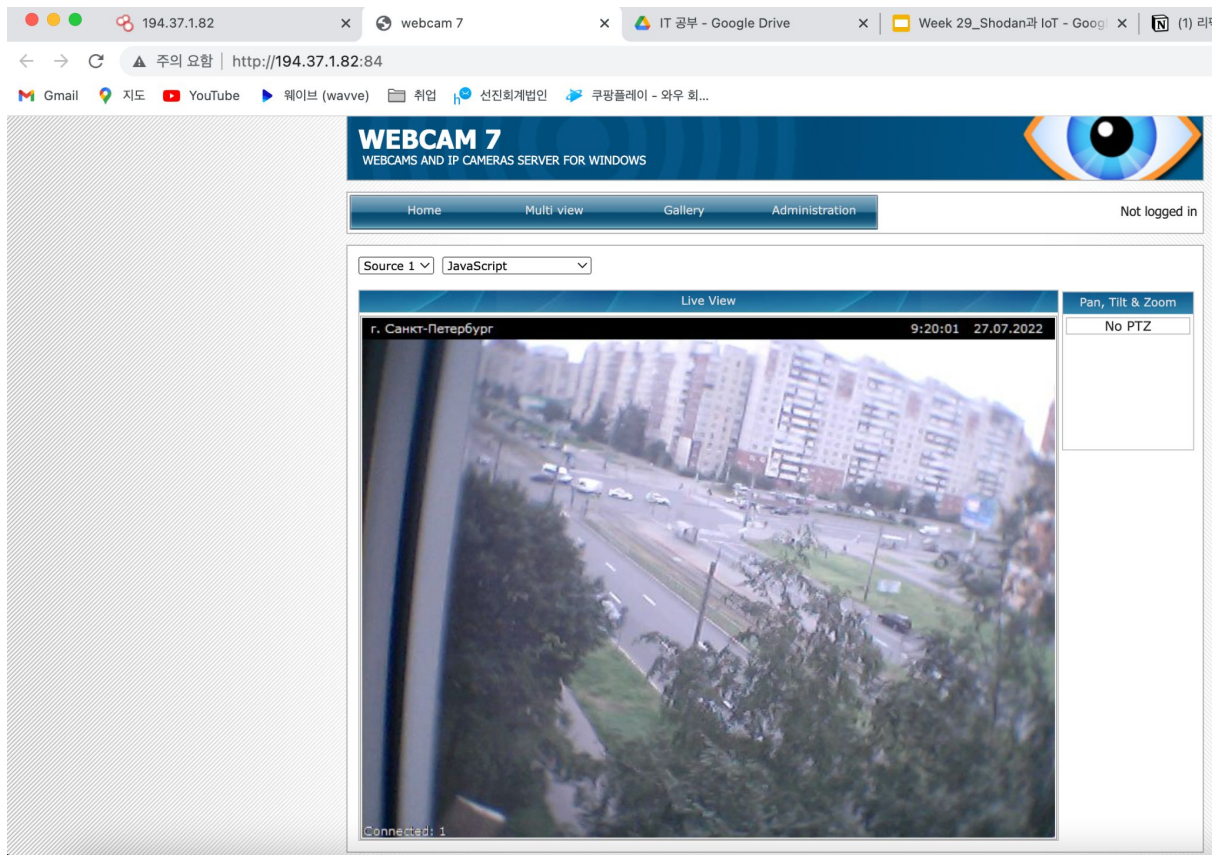
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7224
Cache-control: no-cache, must revalidate
Date: Tue, 26 Jul 2022 15:32:17 GMT
Expires: Tue, 26 Jul 2022 15:32:17 GMT
Pragma: no-cache
Server: **webcam 7**

2022-07-26T15:32:16.450885



г. Санкт-Петербург 18:31:49 26.07.2022

Shodan으로 검색하기 (1) IP 카메라



Shodan으로 검색하기 (1) IP 카메라

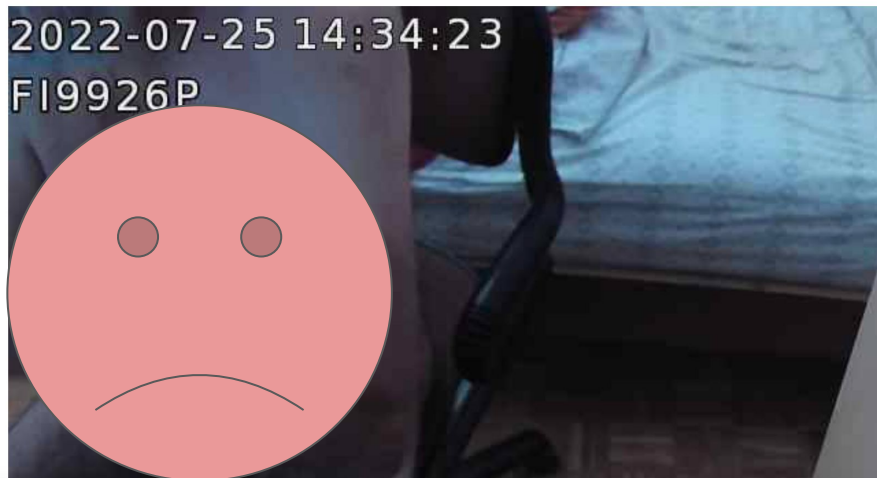
- 비밀번호 없이 공개된 IP 카메라 중 webcamXP(윈도우용 IP 카메라 서버) 찾기
product:"webcamXP httpd"
- * 가정에 설치한 웹캠 화면이 Shodan 크롤러에 수집된 경우. 실제로 접속해서 확인시 서버와 연결할 수 없었습니다

webcamXP 5

82.56.177.10
host-82-56-177-10.retail.t
elecomitalia.it
Telecom Italia S.p.A. TIN
EASY LITE
Italy, Venice

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7518
Cache-control: no-cache, must revalidate
Date: Mon, 25 Jul 2022 14:35:52 GMT
Expires: Mon, 25 Jul 2022 14:35:52 GMT
Pragma: no-cache
Server: webcamXP 5

2022-07-25T14:35:53.797164



Shodan으로 검색하기 (1) IP 카메라

- “하이크비전”사의 웹캠 기본 포트를 검색하여 스크린샷을 보고 원하는 웹캠 찾기
has_screenshot: port:80,8000,554

SHODAN

Explore

Downloads

Pricing


has_screenshot: port:80,8000,554

Account

TOTAL RESULTS

99,911

TOP COUNTRIES



Viet Nam	12,765
Taiwan	11,130
Korea, Republic of	8,477
United States	6,913
Russian Federation	5,063

More...

TOP PORTS

554	83,358
80	15,295
8000	1,258

View Report

Download Results

Historical Trend

Browse Images

View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

NETSurveillance WEB

86.1.53.209
cpc86279-nfds17-2-0-cust
464.8-2.cable.virginm.net
[NORTHFIELDS](#)
United Kingdom, Wigston Magna

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httpd 1.0.0
Expires: 0



2022-07-27T02:49:16.662368

네트워크 프린터의 특징

- 네트워크 프린터란? : 네트워크에 연결된 프린터로, 프린터를 PC에 직접 연결할 필요가 없어 PC당 프린터를 구비할 필요가 없다는 이점이 있음
- 네트워크 프린터의 프로토콜 : LPD, RAW, IPP
- **LPD(Line Printer Daemon protocol)**
 - LPD은 인쇄할 내용을 전송 후 전송 여부를 확인 O, 즉 양방향성.
 - BSD Unix가 있었던 시절부터 있던 프로토콜로, 호환성이 좋음. UNIX 용으로 제작되었으나 후에 다른 platform도 호환이 되도록 발전 → 대부분의 프린터 기기에서 LPD를 지원
 - TCP / IP 및 LPD(Line Printer Deamon)을 이용하여 작동
 - LPD는 문서나 다른 자료를 인쇄할 수 있도록 하는 소프트웨어
 - 디폴트 Port로 515번을 사용함

네트워크 프린터의 특징

- **RAW**

- RAW 프로토콜 : 어느 특정한 프로토콜 전용의 전송 계층 포매팅 없이 패킷을 직접적으로 주고 받게 해주는 소켓. 패킷의 헤더를 직접 제어할 수 있고, 응용 계층과 전송 계층, 네트워크 계층에서 모두 접근이 가능함.
→ RAW 프로토콜을 사용하여 프린트할 때에는 9100번 포트를 사용함
- RAW은 인쇄할 내용을 전송 후 전송 여부를 확인 X, 즉 단방향성.
- 주로 컴퓨터 사용자가 텍스트 이상의 복잡한 문서를 인쇄하고자 할 때 사용.
- 대부분의 프린터 설정시 RAW가 기본적으로 설정됨

네트워크 프린터의 특징

- **IPP(Internet Printing Protocol)**

- 인터넷 연결로 프린터를 사용할 수 있게 해주는 프로토콜. 631번 Port와 TCP/IP를 사용, HTTP 서버 Java(TM) Web Console, SSL 프로토콜이 필요
→ 네트워크 프린터의 프로토콜 중 유일하게 보안이 고려된 프로토콜으로, 공격 시도시 연결이 끊어짐
- 모든 프린터가 IPP를 지원하지는 않음
- IPP 프로토콜을 지원하는 프린터도 프린터 자동 검색 후 추가 시 RAW(9100)가 기본적으로 설정됨.
→ MacOS에서는 IPP 프로토콜을 이용하기 위해선 수동으로 IP주소를 통해 추가해줘야 함

- 네트워크 프린터의 보안 취약점 : 네트워크 프린터는 보안 기능을 갖춘 IPP를 사용하지 않거나, 프린터 사용시 인증 기능을 사용하지 않는 경우 보안에 취약점을 가짐.
→ 네트워크를 기반으로 공격하고 있으므로 파급력은 미약하나, vendor에 종속적인 취약점이 아닌 프로토콜에 기반을 둔 취약점임. 따라서 대부분의 네트워크 프린터에서 같은 취약점이 존재함.

Shodan으로 검색하기 (2) 네트워크 프린터

- printer port:515,9100,631
- 검색된 국가 중 1위가 한국, 기관명 1, 2, 4위가 한국임

SHODAN

Explore

Downloads

Pricing


printer port:515,9100,631

Account

TOTAL RESULTS

50,027

TOP COUNTRIES



Korea, Republic of	14,399
United States	8,829
China	3,293
Japan	2,642
Taiwan	2,314

More...

TOP PORTS

515	40,805
631	8,857
9100	365

TOP ORGANIZATIONS

Korea Telecom	9,889
SK Broadband Co Ltd	1,774
NTT DOCOMO,INC.	1,372
LG DACOM Corporation	1,332
Chunghwa Telecom Co.,L...	1,197

View Report

Download Results

Historical Trend

View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

64.139.227.168

Suddenlink Communications

United States, Georgetown

Windows LPD ServerError: specified printer does not exist

2022-07-20T11:37:49.622594

87.5.4.47

host-87-5-4-47.retail.telcomitalia.it

Telecom Italia S.p.A.

TIN EASY LITE

Italy, Brescia

Unable to get printer printer: successful-ok

2022-07-20T11:37:27.219281

Not Found - CUPS v1.5.4

76.14.176.108

76-14-176-108.wsac.wavecable.com

Wave Broadband

United States, San Francisco

HTTP/1.1 404 Not Found

Date: Fri, 29 Jul 2022 11:37:16 GMT

Server: CUPS/1.5

Content-Language: en_US

Connection: close

Content-Type: text/html; charset=utf-8

Content-Length: 342

CUPS (IPP):

Printer #1:

Make And Model: HP Business Inkjet 2200 - CUPS+Gutenprint v5.2.10

Name: HPPR...

2022-07-20T11:37:16.392577

222.107.52.164

Korea Telecom

Korea, Republic of, Seoul

Windows LPD ServerError: specified printer does not exist

2022-07-20T11:36:48.943596

Shodan으로 검색하기 (2) 네트워크 프린터

- 515번 포트가 열려 있는 IP 중 하나.
구체적인 기종도 확인 가능

47.110.23.219 Regular View Raw Data History Hangzhou

// TAGS: videogame // LAST SEEN: 2022-0

General Information

Country	China
City	Hangzhou
Organization	Aliyun Computing Co., LTD
ISP	Hangzhou Alibaba Advertising Co.,Ltd.
ASN	AS37963

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

Open Ports

13	17	19	21	25	26	37	49	51
53	70	80	82	83	86	99	102	104
111	113	119	131	143	195	221	225	444
465	502	503	515	548	554	587	636	666
771	789	800	843	873	902	943	992	995
1000	1099	1153	1177	1200	1234	1290	1344	1400
1433	1500	1515	1521	1599	1650	1741	1830	1833

// **515** / TCP 2115448635 | 2022-07-29T11:38:12,387976

Toshiba e-STUDIO 233 copier/printer/fax http config