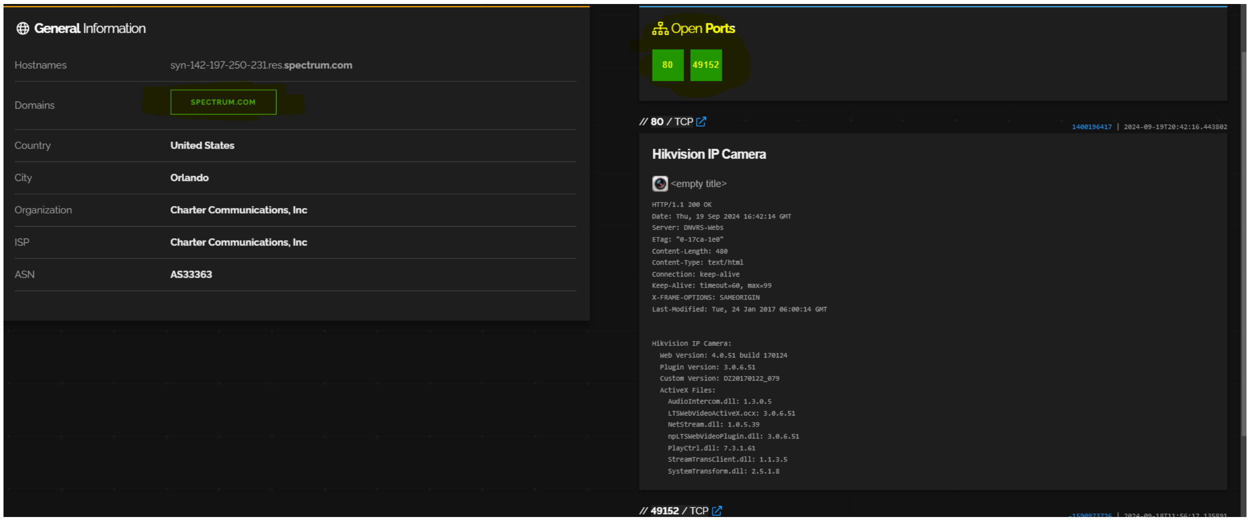
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing Fall
2024

Assignment 1: Passive Reconnaissance

Handout Date: September 12, 2024
Due Date: September 20, 2024 11:59 pm
Total Points: 30

Question 1: Login to Shodan (https://www.shodan.io/) using your Gmail account or any other account you have created with the portal. Search ***Web Camera*** or ***Web Cam*** in the search bar and you will be shown a report where a number of accessible web cameras are listed.

Task 1: Go through each link with the tag **WEB SERVICE** until you find a device where there is at least one open port and the domain name (URL) is displayed. If you find multiple such devices, just choose one arbitrarily. Take a screenshot highlighting the domain name and the open ports. Attach the screenshot in your submission. **4 points**



General Information

Hostnames	syn-142-197-250-231.res.spectrum.com
Domains	SPECTRUM.COM
Country	United States
City	Orlando
Organization	Charter Communications, Inc
ISP	Charter Communications, Inc
ASN	AS33363

Open Ports

80 49152

// 80 / TCP 1400196417 | 2024-09-19T20:42:16.443802

Hikvision IP Camera

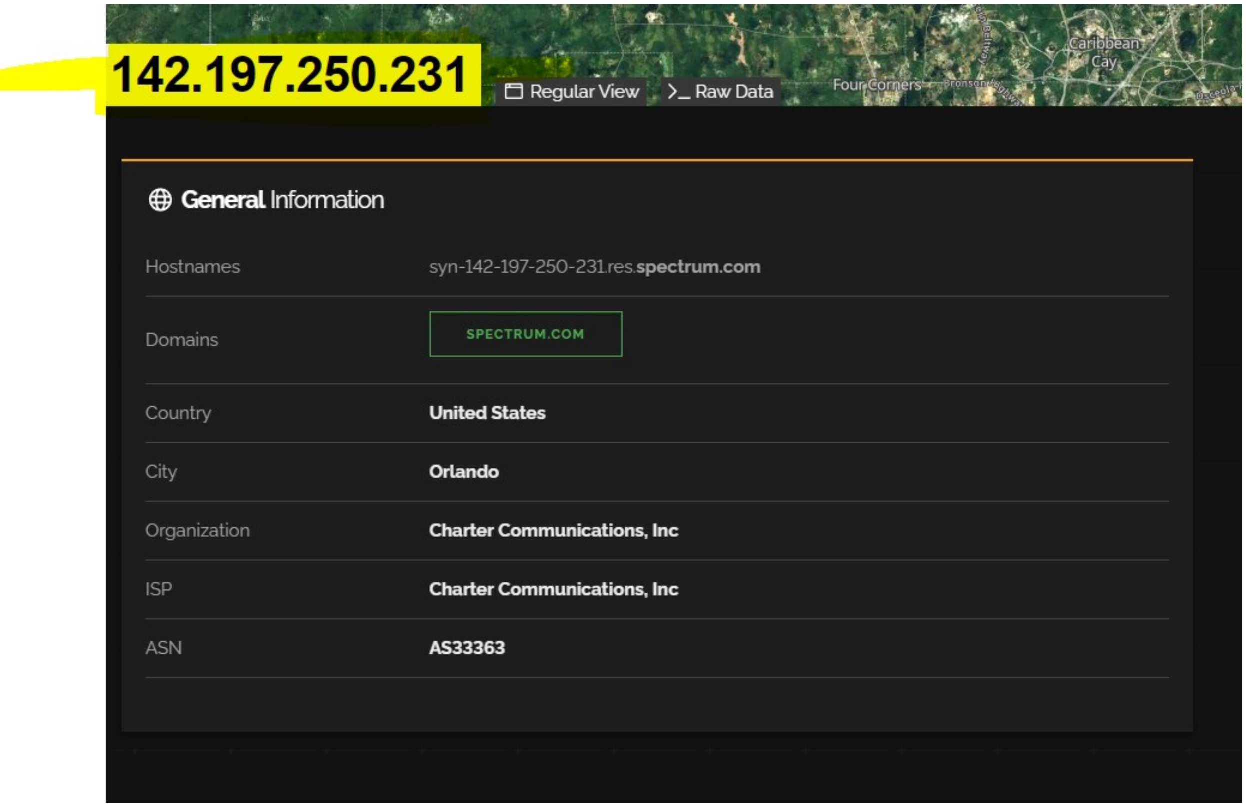
<empty title>

```
HTTP/1.1 200 OK
Date: Thu, 19 Sep 2024 16:42:14 GMT
Server: DNVRS-Webs
ETag: "0-17ca-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
X-FRAME-OPTIONS: SAMEORIGIN
Last-Modified: Tue, 24 Jan 2017 06:00:14 GMT


Hikvision IP Camera:
  Web Version: 4.0.51 build 170124
  Plugin Version: 3.0.6.51
  Custom Version: DZ20170122_079
  ActiveX Files:
    AudioIntercom.dll: 1.3.0.5
    LTSWebVideoActiveX.ocx: 3.0.6.51
    NetStream.dll: 1.0.5.39
    npLTSWebVideoPlugin.dll: 3.0.6.51
    PlayCtrl.dll: 7.3.1.61
    StreamTransClient.dll: 1.1.3.5
    SystemTransform.dll: 2.5.1.8
```

// 49152 / TCP -1590973726 | 2024-09-18T11:56:17.135891

- **Task 2**: Using WHOIS (https://who.is/) or Netcraft (_), find the IP address of the domain name you found in Task 1. Take a screenshot highlighting the IP address and attach it in your submission. Go through the complete report you retrieved from WHOIS or Netcraft. Do some research online about the vulnerabilities or weakness the device has. Briefly describe all the security weakness or vulnerabilities you found. **6 points**



142.197.250.231

General Information

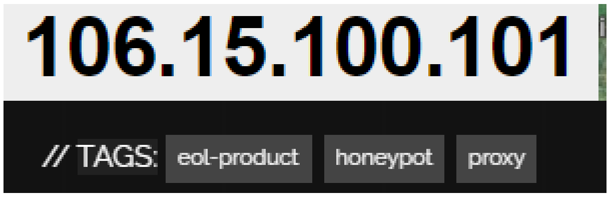
Hostnames	syn-142-197-250-231.res.spectrum.com
Domains	SPECTRUM.COM
Country	United States
City	Orlando
Organization	Charter Communications, Inc
ISP	Charter Communications, Inc
ASN	AS33363

A big vulnerability that could be exploited is that the device uses JavaScript. While JavaScript is used by a variety of devices and companies it is also known for being vulnerable to multiple attacks. Some being input validation and unintended script execution. For example, an attack used against a JavaScript system took advantage of being able to embed malicious code on the clients end of the website which would then steal and route data back to the hacker.

Question 2: Login to Shodan again, but this time search for ***port:502***. Select a device that meets the following criteria:

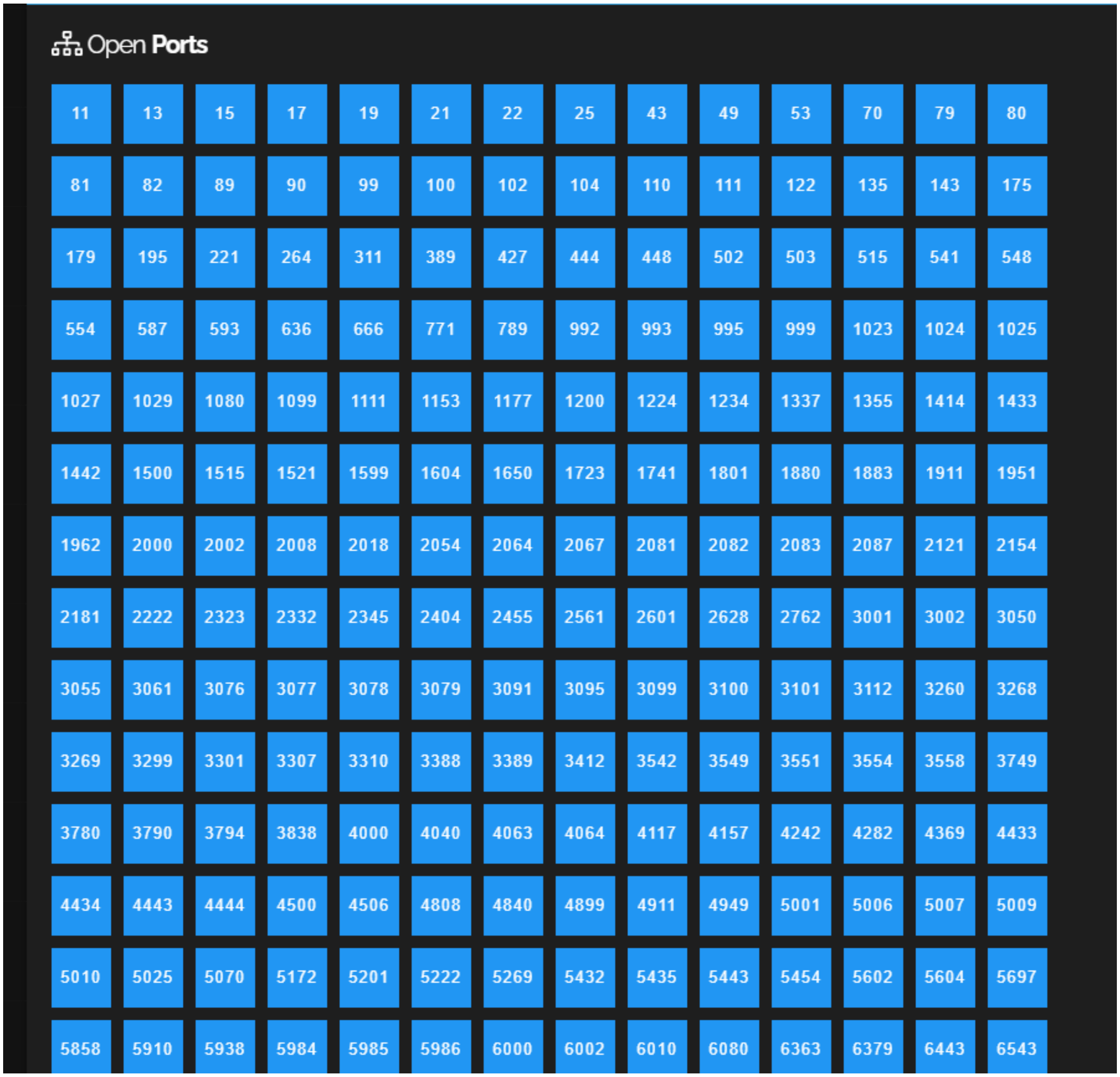
1. There is at least some information in the ***device identification*** field.
2. There is at least one **CVE** listed in the ***Vulnerabilities*** section.

- **Task 1**: Capture some screenshots showing the device id, open ports, and the CVE lists. Attach the screenshots in your submission. **5 points**



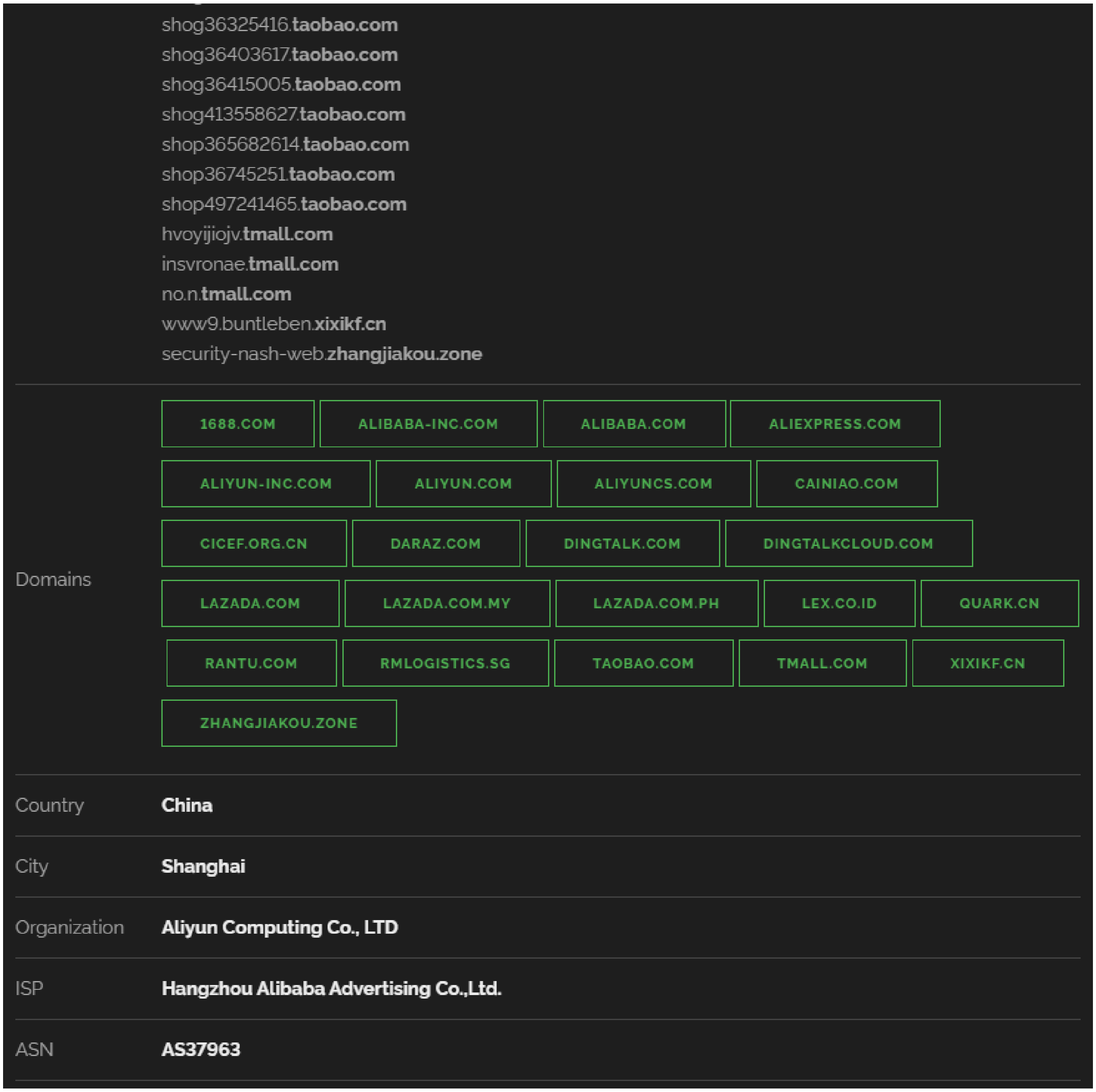
106.15.100.101

// TAGS: eol-product honeypot proxy



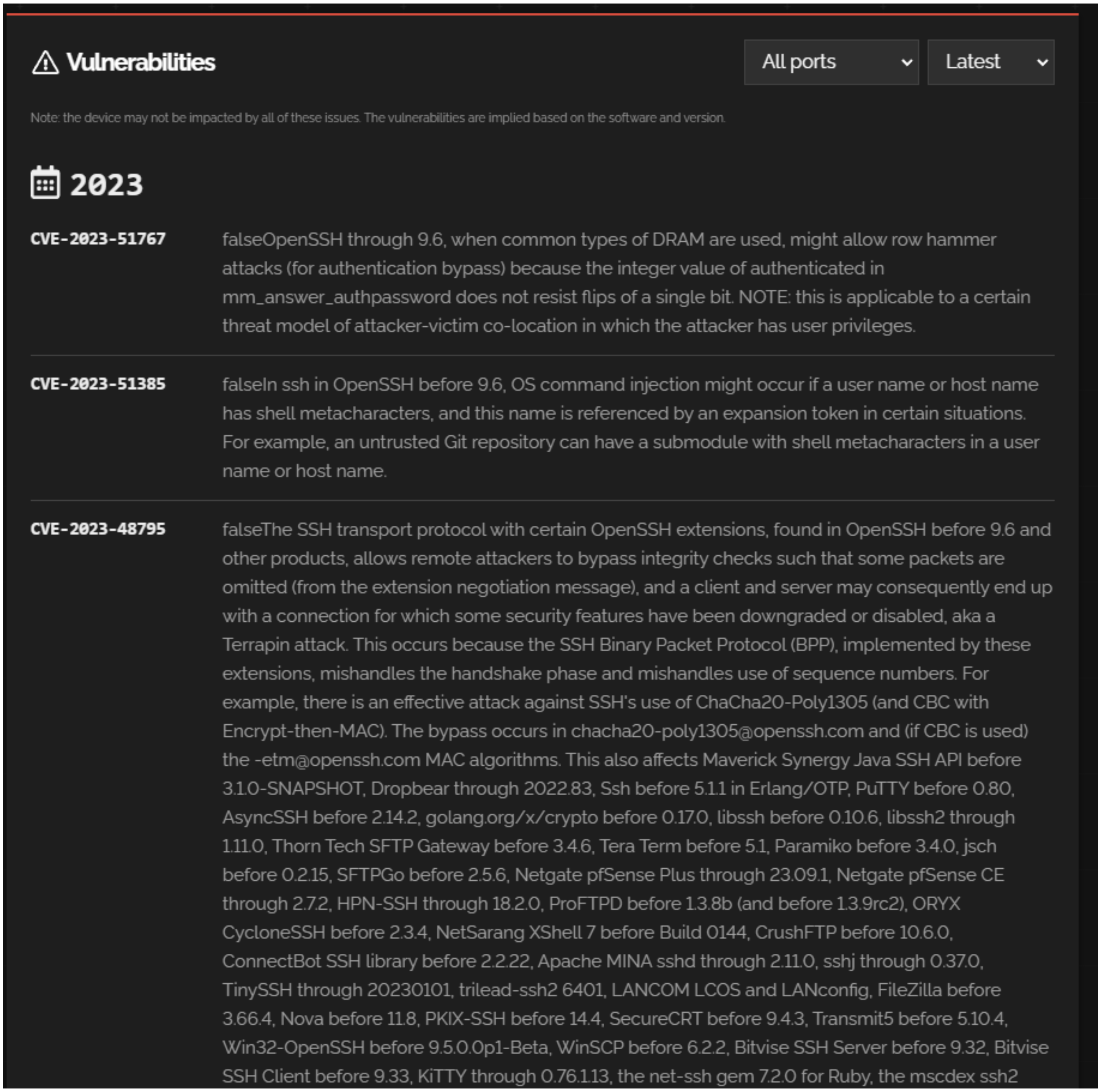
Open **Ports**

11	13	15	17	19	21	22	25	43	49	53	70	79	80
81	82	89	90	99	100	102	104	110	111	122	135	143	175
179	195	221	264	311	389	427	444	448	502	503	515	541	548
554	587	593	636	666	771	789	992	993	995	999	1023	1024	1025
1027	1029	1080	1099	1111	1153	1177	1200	1224	1234	1337	1355	1414	1433
1442	1500	1515	1521	1599	1604	1650	1723	1741	1801	1880	1883	1911	1951
1962	2000	2002	2008	2018	2054	2064	2067	2081	2082	2083	2087	2121	2154
2181	2222	2323	2332	2345	2404	2455	2561	2601	2628	2762	3001	3002	3050
3055	3061	3076	3077	3078	3079	3091	3095	3099	3100	3101	3112	3260	3268
3269	3299	3301	3307	3310	3388	3389	3412	3542	3549	3551	3554	3558	3749
3780	3790	3794	3838	4000	4040	4063	4064	4117	4157	4242	4282	4369	4433
4434	4443	4444	4500	4506	4808	4840	4899	4911	4949	5001	5006	5007	5009
5010	5025	5070	5172	5201	5222	5269	5432	5435	5443	5454	5602	5604	5697
5858	5910	5938	5984	5985	5986	6000	6002	6010	6080	6363	6379	6443	6543



shog36325416.**taobao.com**
shog36403617.**taobao.com**
shog36415005.**taobao.com**
shog413558627.**taobao.com**
shop365682614.**taobao.com**
shop36745251.**taobao.com**
shop497241465.**taobao.com**
hvoyijiojv.**tmall.com**
insvronae.**tmall.com**
no.n.**tmall.com**
www9.buntleben.**xixikf.cn**
security-nash-web.**zhangjiakou.zone**

Domains	1688.COM ALIBABA-INC.COM ALIBABA.COM ALIEXPRESS.COM ALIYUN-INC.COM ALIYUN.COM ALIYUNCS.COM CAINIAO.COM CICEF.ORG.CN DARAZ.COM DINGTALK.COM DINGTALKCLOUD.COM LAZADA.COM LAZADA.COM.MY LAZADA.COM.PH LEX.CO.ID QUARK.CN RANTU.COM RMLOGISTICS.SG TAOBAO.COM TMALL.COM XIXIKF.CN ZHANGJIAKOU.ZONE
Country	**China**
City	**Shanghai**
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.

2023

CVE-2023-51767 falseOpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

CVE-2023-51385 falseIn ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

CVE-2023-48795 falseThe SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2

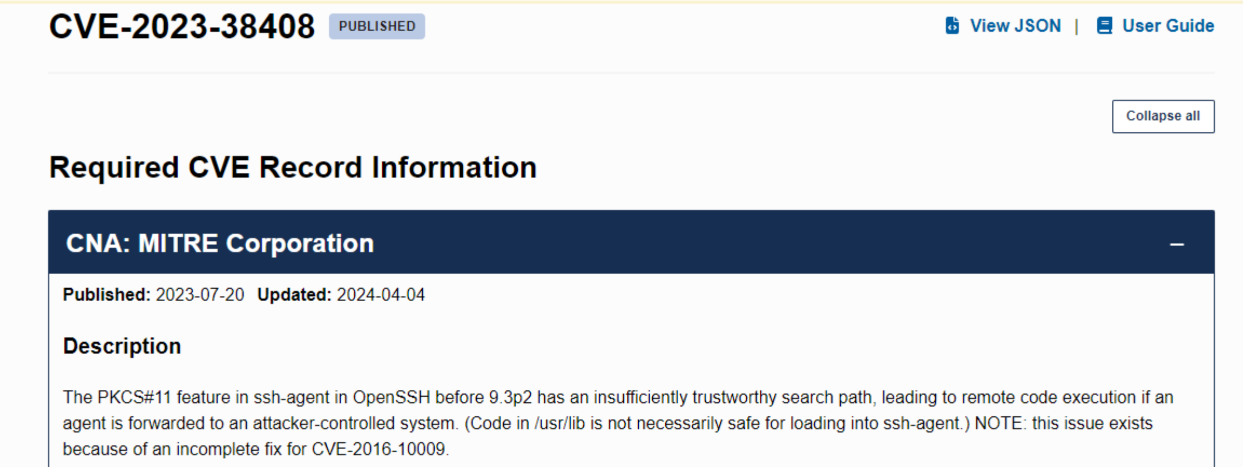
- **Task 2**: Do some research about the device you chose and describe the device type and found vulnerabilities in a paragraph. Try to keep the paragraph limited into 5-10 sentences. **5 points**

After doing some research on the device I found that due to it being connected to so many domains and different companies the device is most likely a server. This was further confirmed by visiting one of the websites ran by the server known as Alibaba. While looking into some of the common vulnerabilities this server could be affected by their seemed to be common trends. This is due to OpenSSH that is used by the server. By exploiting how the server achieves connection attackers can execute remote code. A simple vulnerability occurred that allowed hackers to be able to inject into the OS command if their username had shell metacharacters.

Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing Fall
2024

- **Task 3**: Select a CVE from the CVE list shown in the *Vulnerabilities* section and search for that CVE in https://cve.mitre.org/. Identify the attack/vulnerability described in the CVE. Go to https://attack.mitre.org/matrices/enterprise/network/ and find the attack from the matrix. If the attack is not listed there, try to search in other attack matrices given in the MITRE ATT&CK website. Once you find the attack listed as a ***technique***, try to find out one relevant ***detection*** and one ***mitigation*** methods. Take screenshots showing the detection id and the mitigation id. Attach your screenshots in your submission and briefly summarize the selected detection and mitigation methods. **10 points**

An attacker could take advantage of OpenSSH and execute code remotely if an agent was sent to a system that the attacker already had control of.



CVE-2023-38408 PUBLISHED

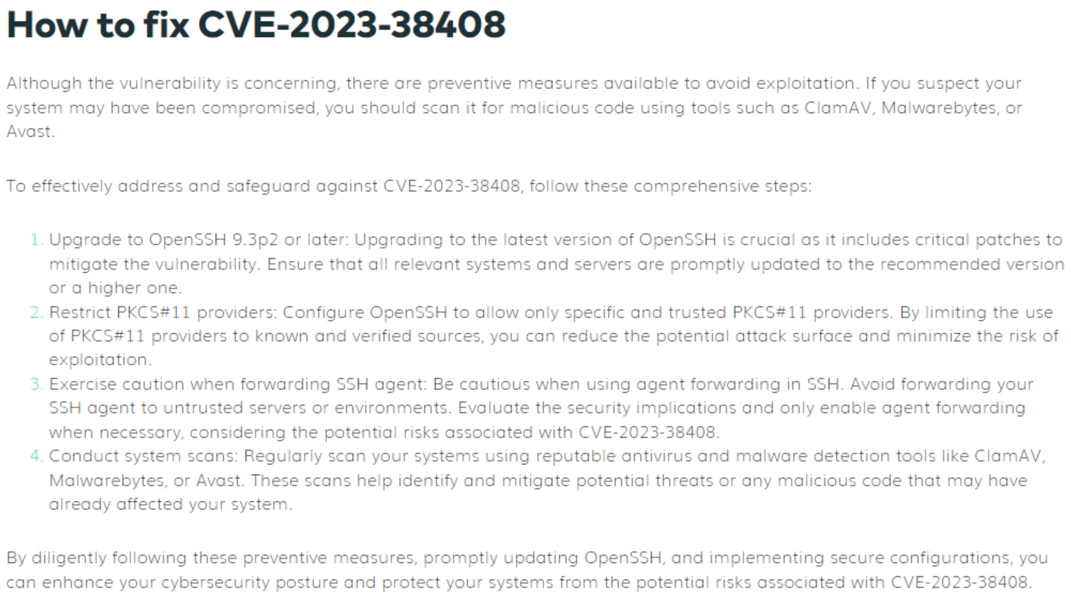
Required CVE Record Information

CNA: MITRE Corporation

Published: 2023-07-20 **Updated:** 2024-04-04

Description

The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.



How to fix CVE-2023-38408

Although the vulnerability is concerning, there are preventive measures available to avoid exploitation. If you suspect your system may have been compromised, you should scan it for malicious code using tools such as ClamAV, Malwarebytes, or Avast.

To effectively address and safeguard against CVE-2023-38408, follow these comprehensive steps:

1. Upgrade to OpenSSH 9.3p2 or later: Upgrading to the latest version of OpenSSH is crucial as it includes critical patches to mitigate the vulnerability. Ensure that all relevant systems and servers are promptly updated to the recommended version or a higher one.
2. Restrict PKCS#11 providers: Configure OpenSSH to allow only specific and trusted PKCS#11 providers. By limiting the use of PKCS#11 providers to known and verified sources, you can reduce the potential attack surface and minimize the risk of exploitation.
3. Exercise caution when forwarding SSH agent: Be cautious when using agent forwarding in SSH. Avoid forwarding your SSH agent to untrusted servers or environments. Evaluate the security implications and only enable agent forwarding when necessary, considering the potential risks associated with CVE-2023-38408.
4. Conduct system scans: Regularly scan your systems using reputable antivirus and malware detection tools like ClamAV, Malwarebytes, or Avast. These scans help identify and mitigate potential threats or any malicious code that may have already affected your system.

By diligently following these preventive measures, promptly updating OpenSSH, and implementing secure configurations, you can enhance your cybersecurity posture and protect your systems from the potential risks associated with CVE-2023-38408.

To mitigate this vulnerability, it is recommended to update OpenSSH and to configure SSH to only allow specific providers to reduce the attack surface. While this vulnerability has no reports of widespread use in a major case it can be detected by looking at traffic logs and a good IPS programed to look for and flag random libraries being installed, loaded, and unloaded in the system.

References

Divinsky, Yair. "How to Fix CVE-2023-38408 in Openssh." ***Vulcan Cyber*****, 25 Aug. 2024, vulcan.io/blog/how-to-fix-cve-2023-38408-in-openssh/.**