Flags To CVEs

Moving From CTFs To Real-World Targets

TABLE OF CONTENTS

Ø1

Intro

whoami

Jack Maginnes (@_stigward)

- Senior Vulnerability Researcher @ Interrupt Labs
- Creator of exploits.club
- Snowboarding & Triathlon

On The Shoulders Of Giants

How Do You Actually Find Bugs? by Mark Dowd

The Layman's Guide To Zero Day Engineering by Markus Gaasedelen and itszn

Attacking Chrome IPC by Ned Williamson

From CTFs To Real World by DayZeroSec Podcast

Motivation

- Most Commonly Asked Question
- Most Commonly Missed Interview Question
- Biggest Hurdle For New Researchers

Scope

- Mainly Low-Level Application Security
- Mindset and Ideas Will Be Transferable

02

Major Differences

Major Differences

- Size
- Complexity
- Attack Surface
- Mindset

(Potentially) Missing Skills

- Attack Surface Enumeration
- Time Management
- Automation and Tool Dev

AVOID THE PITFALL

- "I can't move to looking at real targets until I learn X"

Ø3

Making The Shift

General Tactics

Read...A Lot

Read Write-Ups, Papers, Blogs

Learn *How* To Read Effectively

Build A Note Taking Workflow

Where To Find Materials To Read

- X / Twitter
- Build a personal feed (RSS, Feedly, etc)
- Newsletters
- Company Slack Channels
- Use a read-it-later app (Reader, Raindrop, Pocket, etc)

How To Read Effectively

- How To Read A Research Paper
- You don't need to fully understand all of it
- Highlight / take notes
- Add references to read-later

See Something Interesting

Save To Read It Later App

Read And Highlight

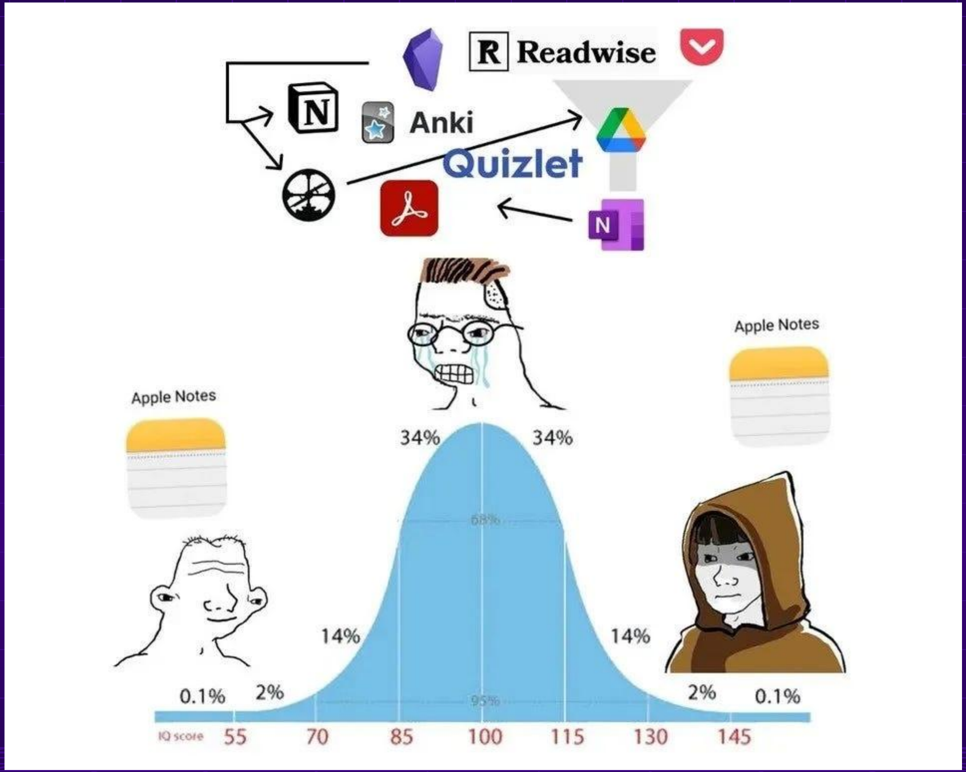
Transfer to note taking app

Mini essay

Down The Rabbit Hole...

- How To Take Smart Notes
- Building a Second Brain
- Obsidian, Taming a Collective Consciousness
- Hacking Your Brain With Obsidian
- Maps of Content – Organize and Think with MOCs 💭
- Use A Work Journal To Recover Focus Faster And Clarify Your Thoughts

Down The Rabbit Hole...



AVOID THE PITFALL

- Notes / Reading Are Helpful....BUT
  - Should not come at the expense of time you could be hacking
  - Organizing a KM system can be a means of procrastination in & of itself
- Set dedicated start / end times

The Other Case For Notes

"I'm making no progress"

- Progress is good
  - Document how a subsystem works – look at what you now understand!
  - Draw a diagram
  - Write a tool
  - Go outside
- If you fail – keep an eye on future vulns for that target. Why did you miss them?

Tools For The Toolbox

Tools For The Toolbox

- Learn The Fundamentals Of Fuzzing
- Pick a Static Analysis Tool (Semgrep, CodeQL, Weggli)
- Trail of Bits Testing Handbook
- Know their uses – don't over-rely

What Should I Work On?

[redacted] Yesterday at 8:54 PM

Just a weird question how do you pick an app to do VR on??

Like is it useful to pick something major? or should I be aiming for small application people don't know about

Good First Projects

- 1-day / N-Day Exploits
- Soft Targets
- Realistic CTF Challenges In The Direction You Want To Progress

Project Selection

- Interesting To You
- 10% Above Your Skill Level

04

Case Studies

1-Day Exploit

CVE-2023-35138

How To Pick A CVE?

Vendor, Product, CVE, ...

HOME ENTRIES PR

LOW ระบบ

Recent

Updates

Archive

Vendor

Product

Type

Stats

Updates

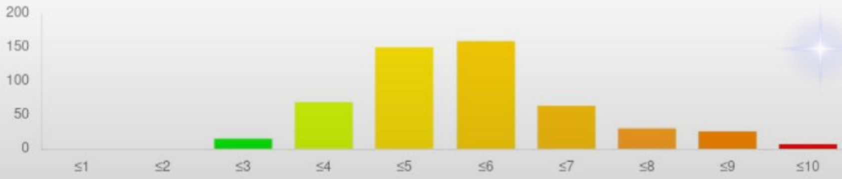
If the moderation team detects changes of existing vulnerabilities or new data of existing vulnerabilities are getting published, the old entries will be updated. This happens if needed and on a regular basis which concludes in a maximum of data quality. Every entry contains a timestamp of the last update and a change log of updated fields. Please use the edit feature to commit updates to existing entries.

- LOW Ziteboard Online Whiteboard Plugin Shortcode cross site scripting
- LOW ImageMapper Plugin imgmap_delete_area_ajax authorization
- LOW Bitly Plugin Shortcode cross site scripting
- MEDIUM WD WidgetTwitter Plugin Shortcode sql injection
- LOW MyBB Theme Management cross site scripting

CVSS Current Top

Top vulnerabilities with the highest CVSSv3 temp scores at the moment. The score is generated by separate values which are called vectors. Those vectors define the structure of the vulnerability. They rely on attack prerequisites and impact. The calculated score ranges between 0.0 and 10.0 whereas a high value declares a high risk. The main score is the base score which analyses the structure of the vulnerability only. The extended score called temp score introduces time-based aspects like exploit and countermeasure availability. Our moderators classify every entry to generate a CVSS score as accurate as posible.

- 9.8 ~~Zyxel NAS326/NAS542 WSGI Server os command injection~~
- 9.8 Zyxel NAS326/NAS542 HTTP POST Request show_zysync_server_contents os command injection
- 9.8 ~~Zyxel NAS326/NAS542 Web Server os command injection~~
- 9.6 Netgear ProSAFE Network Management System Java Debug Wire Protocol missing authentication
- 9.4 Delta Electronics InfraSuite Device Master UDP Packet routine



Exploit Price Current Top

Top vulnerabilities with the highest exploit price at the moment. These price estimations are calculated prices based on mathematical algorithm. This algorithm got developed by our speci exploit market structure and exchange behavior of involved actors. It allows the prediction of generic prices by considering multiple technical aspects of the affected vulnerability. The more tec the accuracy of the reproducable approximation.

How To Pick A CVE?

CVE-2023-35138

A command injection vulnerability in the "show_zysync_server_contents" function in Zyxel NAS devices could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.

- Function Name ✅
- Vulnerability Type ✅
- Entry Point ✅

How To Pick A CVE?

- Firmware ✅

Material	Version	OS	Language	Release Date	Download	Checksum
Firmware	V5.21(AAZF.15)C0		English	November 16, 2023		
Declaration	007.214-01-00591		English	August 31, 2023		
Firmware	V5.21(AAZF.14)C0		English	June 16, 2023		
Firmware	V5.21(AAZF.13)C0		English	May 25, 2023		
User's Guide	V5.21_Ed4		English	August 11, 2022		
Datasheet	6		English	July 04, 2022		
Battery Document	1		English	June 21, 2021		

CVE-2023-35138

- Download vulnerable firmware
- Binwalk
- Grep

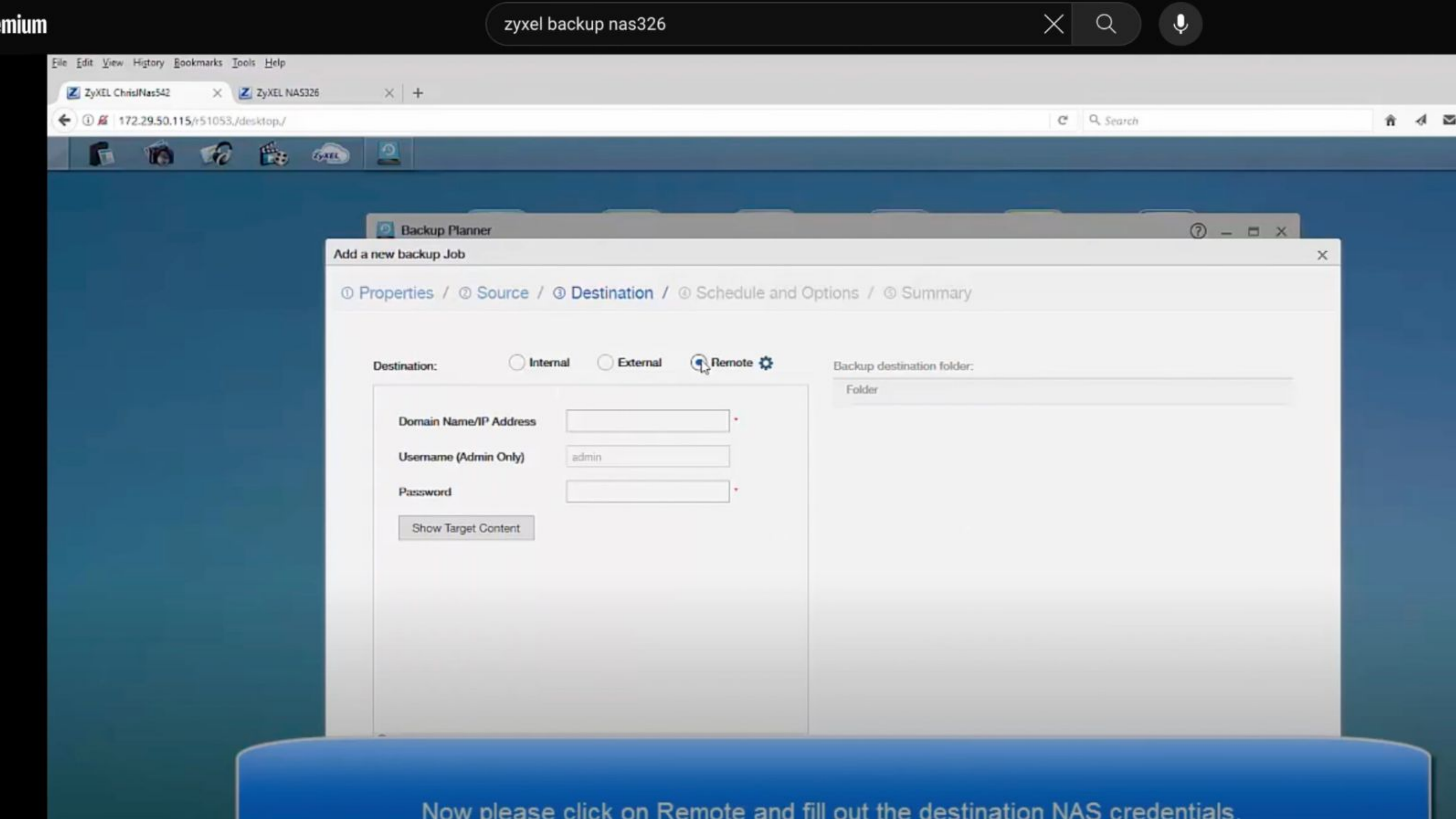
```
stigward@stigward-virtual-machine:~/Desktop/Projects/Nday_Video/full_fs$ rg "show_zysync_serve
r_contents"
usr/local/apache/htdocs/desktop,/utility/command.js
120:      getRemoteServerContent:'/cmd,/ck6fup6/BackupPlanner_main/show_zysync_server_contents',

usr/local/apache/htdocs/desktop,/script/BkupBackupAdd.js
970:                          store.proxy.url = '/cmd,/ck6fup6/BackupPlanner_main/show_zysync_server
_contents';
stigward@stigward-virtual-machine:~/Desktop/Projects/Nday_Video/full_fs$
```

CVE-2023-35138

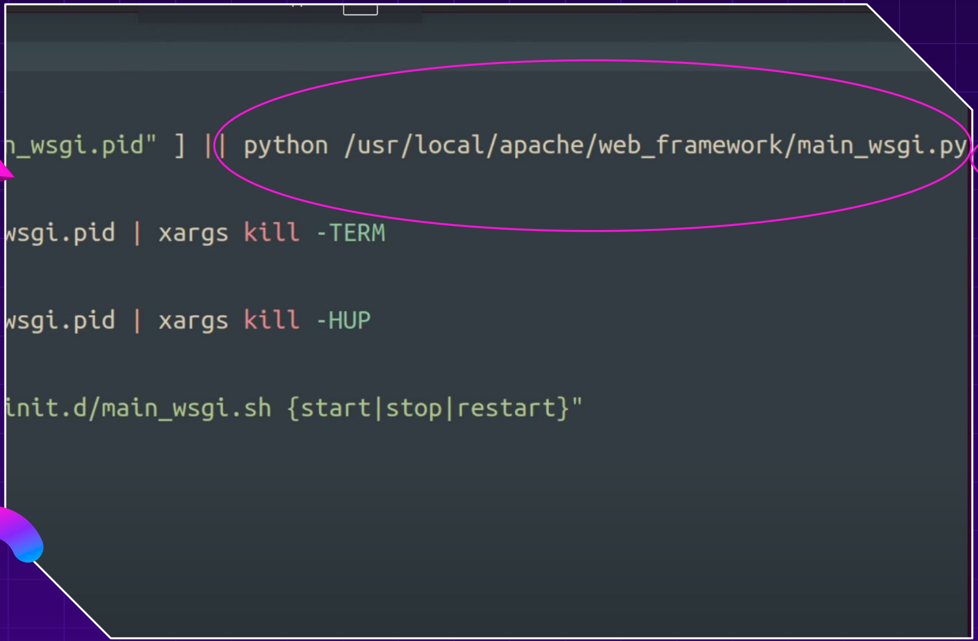
```
stigward@stigward-virtual-machine:~/Desktop/Projects/Nday_Video/full_fs$ rg getRemoteServerCon
tent
usr/local/apache/htdocs/desktop,/utility/command.js
120:      getRemoteServerContent:'/cmd,/ck6fup6/BackupPlanner_main/show_zysync_server_contents',

usr/local/apache/htdocs/desktop,/script/BkupBackupAdd.js
1481:                          url:"getRemoteServerContent",
```

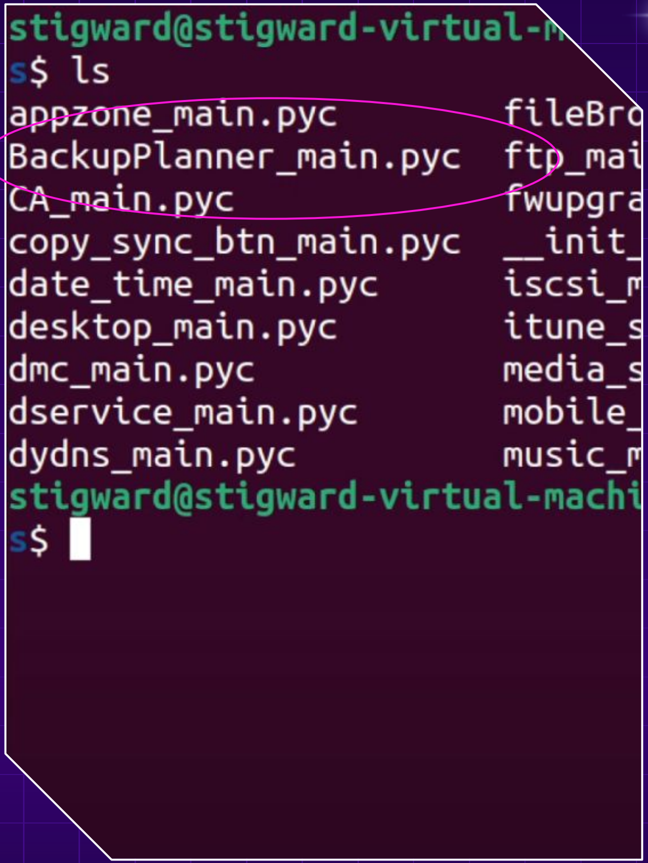
CVE-2023-35138

```
showContent:function(){
  this.isConnectSuccess = false;
  Ext.getCmp("connectWarningMsg").removeCls("subWindowText-div-error");
  Ext.getCmp("connectWarningMsg").removeCls("subWindowText-div-success");
  Ext.getCmp("connectWarningMsg").el.dom.innerHTML = '<image src="res/images/loading-smal
  Ext.create('Utility.Ajax',{
    url:"getRemoteServerContent",
    isAddToken:true,
    params:{IP:Ext.getCmp("serverIP").getValue(),Username:Ext.getCmp("userName").getValue
    scope:this,
    successFn:function(obj,me){
      if(Ext.isEmpty(obj) || (obj.volumes && obj.volumes.length == 0)){
        var errorMsg = getText("Failed to connect to remote device.")+" "+getText("Please
        if(Ext.getCmp("syncRadio").getValue())
          errorMsg += " "+getText("Make sure the target device has the latest firmware in
        Ext.getCmp("connectWarningMsg").removeCls("subWindowText-div-success");
        Ext.getCmp("connectWarningMsg").addCls("subWindowText-div-error");
        Ext.getCmp("connectWarningMsg").el.dom.innerHTML = getText("Connection failed.")+
      }
```


emium
zyxel backup nas326
File Edit View History Bookmarks Tools Help
ZyXEL ChrisNas542
ZyXEL NAS326
172.29.50.115/r51053/desktop/
Search
Backup Planner
Add a new backup Job
① Properties / ② Source / ③ Destination / ④ Schedule and Options / ⑤ Summary
Destination:
Internal
External
Remote
Backup destination folder:
Folder
Domain Name/IP Address
Username (Admin Only)
admin
Password
Show Target Content
Now please click on Remote and fill out the destination NAS credentials.

What Handles The Request??





Looking at init script

PREVIOUS PROJECTS

README.markdown

Decompyle++

A Python Byte-code Disassembler/Decompiler

+

GREP.....

PREVIOUS PROJECTS

```
stigward@stigward-virtual-machine:~/Desktop/Projects/Nday_Video/full_fs/usr/local/apache/web_framework$ rg "show_
zysync"
models/BackupPlanner_main_model.py
227:def zysh_show_zysync_server_contents(input):
```

```

def zysh_show_zysync_server_contents(input):
    strcmd = '/usr/bin/zysync --query_rsync_module "%s" "%s" "%s" "%s"' % (input['IP'], input['Username'], i
    retvalue = os.popen(strcmd)
    output = []
```

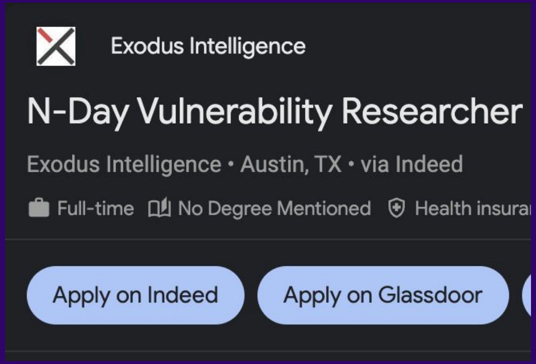
CVE-2023-35138

- Write A Python Reverse Shell
- Craft A Malicious Request
- Profit

CVE-2023-35138

How To Pick A CVE?

- Attack Surface Enumeration ✅
- Vulnerability Identification ✅
- Real Exploitation ✅



And Sometimes...

CVE-2020-14938 - Botched Patch

CVE-2020-14938

CVE-2020-14938 Detail

Description

An issue was discovered in map.c in FreedroidRPG 1.0rc2. It assumes lengths of data sets read from saved game files. It copies data from a file into a fixed-size heap-allocated buffer without size verification, leading to a heap-based buffer overflow.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector string

CVSS 3.x Severity and Vector Strings:

NVD **NIST:** NVD **Base Score:** **9.8 CRITICAL** **Vect**

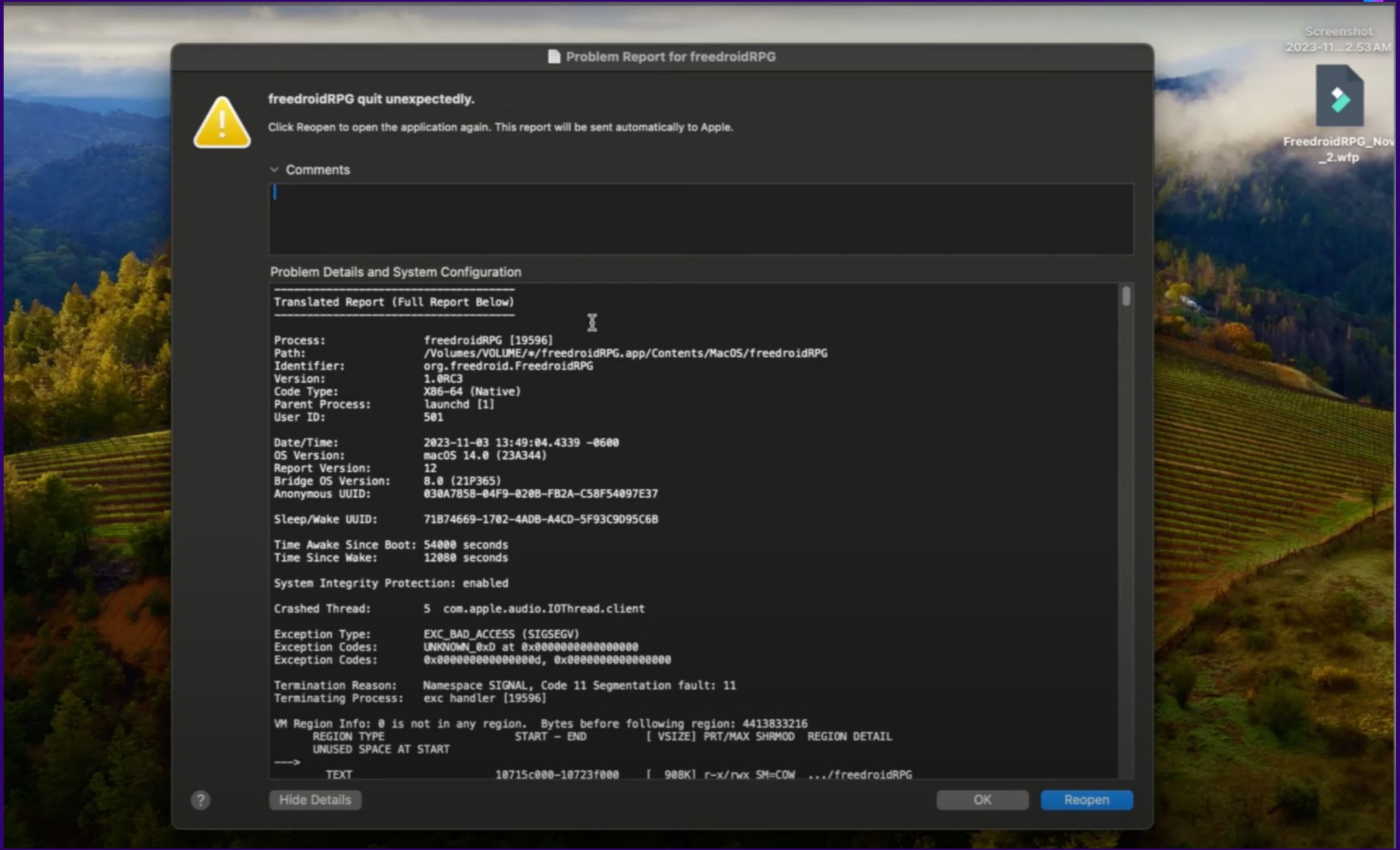
CVE-2020-14938

```diff
         short int nlpos = 0;
-        memset(this_line, 0, 4096);
-        while (wp_begin[curlinepos + nl
+        while (wp_begin[curlinepos + nlpos] != '\n' && (wp_begin + curlinepos + nlpos < wp_end))
             nlpos++;
+
+        if (nlpos > (37+100*4)) { // Enough room for a waypoint with 100 connections
+            error_message(__FUNCTION__,
+                "A very long line has been detected in a waypoint config of the savegame.\n"
+                "Line length: %d chars.\n"
+                "That savegame is probably corrupted, we do not want to load it.",
+                IS_FATAL, nlpos);
+        }
```

Oops...You Found An 0Day

All Fixed...Right?

Full Details Here


Problem Report for freedroidRPG
freedroidRPG quit unexpectedly.
Click Reopen to open the application again. This report will be sent automatically to Apple.
Comments
Problem Details and System Configuration
Translated Report (Full Report Below)
Process: freedroidRPG [19596]
Path: /Volumes/VOLUME/*/freedroidRPG.app/Contents/MacOS/freedroidRPG
Identifier: org.freedroid.FreedroidRPG
Version: 1.0RC3
Code Type: X86-64 (Native)
Parent Process: launchd [1]
User ID: 501
Date/Time: 2023-11-03 13:49:04.4339 -0600
OS Version: macOS 14.0 (23A344)
Report Version: 12
Bridge OS Version: 8.0 (21P365)
Anonymous UUID: 030A7858-04F9-020B-FB2A-C58F54097E37
Sleep/Wake UUID: 71B74669-1702-4ADB-A4CD-5F93C9D95C6B
Time Awake Since Boot: 54000 seconds
Time Since Wake: 12080 seconds
System Integrity Protection: enabled
Crashed Thread: 5 com.apple.audio.IOThread.client
Exception Type: EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: UNKNOWN_0xD at 0x0000000000000000
Exception Codes: 0x000000000000000d, 0x0000000000000000
Termination Reason: Namespace SIGNAL, Code 11 Segmentation fault: 11
Terminating Process: exc handler [19596]
VM Region Info: 0 is not in any region. Bytes before following region: 4413833216
REGION TYPE START - END [VSIZE] PRT/MAX SHRMOD REGION DETAIL
UNUSED SPACE AT START
--->
TEXT 10715c000-10723f000 [908K] r-x/rwx SM=COW .../freedroidRPG
Hide Details
OK
Reopen
Screenshot 2023-11...2.53 AM
FreedroidRPG_Nov_2.wfp

When You Don't Know If There Are Bugs

Target: <REDACTED>

Bring Back 0-days on Stage...Ethically

REDACTED Android Device

- Port scanned an Android device – found it listening on port 60002
- Traced it back to an APK, started reverse engineering it
- Custom P2P web server with path traversal vulnerability

REDACTED Android Device

- End goal – RCE on the device
- During recon:
    - Download updates from company website and put them in a specific location to update the device

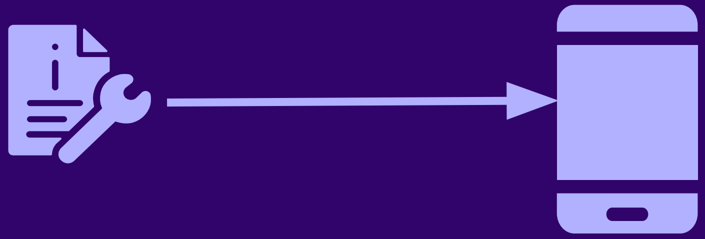
REDACTED Android Device

- What if I use a valid update file and the path traversal? Can I get the device to update?
- No...

REDACTED Android Device

- File is copied – no duplicate file names
- Name *has* to be update.zip to start update

fileName = ./../../../update_dir/update.zip



createFile(/data/data/appname/files/../../update_dir/update.zip)

copyFile(/place/to/copy/../../../update_dir/update.zip)

deleteFile(/data/data/appname/files/../../update_dir/update.zip)

REDACTED Android Device

if (fileName.exists()) {fileName = fileName + "(1)" }

- /update_dir/update.zip is created
- /update_dir/update(1).zip is created
- /update_dir/update.zip is deleted

No update :(

We Need Another Bug

...always assume there is another bug

Race 2 Win

- Reviewed fileName bypasses (null byte injections, playing with extensions)
    - No 🎲
- What about a race condition??

Race 2 Win

Very small, fake update file

Real update file (multiple gigs)

Race 2 Win

Fake update.zip is created

Real update(1).zip is created

Fake update(2).zip is created via copy

Fake update.zip is deleted

Real update.zip is created

Android Firmware is Signed...

...always assume there is another bug

REDACTED Android Device

- Bootloader unlocked
- Used development keys for FW signature

```
$ python3 exploit.py
[+] Starting race 🏎️...
[+] Connecting to server...
[+] Connecting to server...
[+] Dummy file uploaded...
[+] Backdoor uploaded...
[+] Launching listener...
[+] Listening on port 4444
[🏴‍☠️] Connection received from  ('10.0.0.61', 48938)
id
uid=0(root) gid=0(root) groups=0(root) context=u:r:magisk:s0
```

Another Important Takeaway

- Consistency > One Off Time Investment
- Intensity > Volume
- Follow Your Curiosity

THANKS!

Where To Find Me:

https://twitter.com/_stigward

https://blog.exploits.club

https://github.com/stigward