STORMWATCH

CYBERSECURITY NEWS

Dateline: 2024-04-23

LIKE

SUBSCRIBE

Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (https://www.greynoise.io), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

https://StormWatch.ing

LEAVE A COMMENT

SHARE

STORM WATCH

CYBERSECURITY NEWS

CYBERSIDE CHAT

View | Attach (1) | Info | More...

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=24

This is version 24. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes.

All prior versions of CrushFTP were also affected by this most recent vulnerability.
CrushFTP v10 info: https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update

This particular version was published on 19-Apr-2024 04:58 by Ben Spink.

View | Attach (1) | Info | More...

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=25

This is version 25. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes. (CREDIT:Simon Garrelou, of Airbus CERT)

All prior versions of CrushFTP were also affected by this most recent vulnerability.
CrushFTP v10 info: https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update

This particular version was published on 19-Apr-2024 05:27 by Ben Spink.

⚠ This is version 24. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update&version=24

Minimum safe CrushFTP version is 10.7.1. (Regularly updating is critical and we make that as easy as possible.)

Regarding 10.7.1 and the CrushFTP exploit allowing access to system files....using a DMZ in front of your main CrushFTP would have protected you in this scenario. The vulnerability allowed an attacker to retrieve system files.

REGARDING 10.6.0 and the recent global SSH vulnerability which also affected CrushFTP! (not CrushFTP specific, but we are affected just like ALL other server vendors): CVE-2023-48795

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=26

April 19th, 2024
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes. (CREDIT:Simon Garrelou, of Airbus CERT)

IMPORTANT: due to the security updates since CrushFTP version 10.5.2+ any JDBC driver jar file needs to be placed into the CrushFTP10/plugins/lib/ directory, or it won't load. In case of a server previously configured using an external SQL user DB, this new feature prevents access on next launch, will need to

Updating an old CrushFTP v9

You must upgrade: CrushFTPUpgrade
You need a v10+ license code first! If you are an enterprise customer, contact us for your code. Its free if your maintenance is current.

All prior versions of CrushFTP were also affected by this most recent vulnerability.
CrushFTP v10 info: https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=28

This is version 28. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes. (CREDIT:Simon Garrelou, of Airbus CERT)

⚠ This is version 30. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024 https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=30

CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes. (CREDIT:Simon Garrelou, of Airbus CERT)

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for.
•If I have a DMZ am I really safe? Sort of...the attacker could steal files from the DMZ, but the DMZ shouldn't have files...no users, no private keys, no data files, etc...still some OS files, but there shouldn't be anything of real interest.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

April 19th, 2024 https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=31

CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are protected with its protocol translation system it utilizes. (CREDIT:Simon Garrelou, of Airbus CERT)

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for. Possibly looking for "paths=%3CINCLUDE" might be an indicator.
•If I have a DMZ am I really safe? Sort of...the attacker could steal files from the DMZ, but the DMZ shouldn't have files...no users, no private keys, no data files, etc...still some OS files, but there shouldn't be anything of real interest.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=32

April 19th, 2024
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are partially protected with its protocol translation system it utilizes. A DMZ however does not fully protect you and you must update immediately. (CREDIT:Simon Garrelou, of Airbus CERT)

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for. Possibly looking for "paths=%3CINCLUDE" might be an indicator.
•If I have a DMZ am I safe? NO! As of April 22, we have changed our opinion on this. A DMZ does not fully protect you.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

⚠ This is version 33. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024 - CVE-2024-4040
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are partially protected with its protocol translation system it utilizes. A DMZ however does not fully protect you and you must update immediately. (CREDIT:Simon Garrelou, of Airbus CERT)

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=33

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for. Possibly looking for "paths=%3CINCLUDE" might be an indicator.
•If I have a DMZ am I safe? NO! As of April 22, we have changed our opinion on this. A DMZ does not fully protect you.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

⚠ This is version 33. It is not the current version, and thus it cannot be edited.
[Back to current version] [Restore this version]

April 19th, 2024 - CVE-2024-4040
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are partially protected with its protocol translation system it utilizes. A DMZ however does not fully protect you and you must update immediately. (CREDIT:Simon Garrelou, of Airbus CERT)

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=33

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for. Possibly looking for "paths=%3CINCLUDE" might be an indicator.
•If I have a DMZ am I safe? NO! As of April 22, we have changed our opinion on this. A DMZ does not fully protect you.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

April 19th, 2024 - CVE-2024-4040
CrushFTP v11 versions below 11.1 have a vulnerability where users can escape their VFS and download system files. This has been patched in v11.1.0. Customers using a DMZ in front of their main CrushFTP instance are partially protected with its protocol translation system it utilizes. A DMZ however does not fully protect you and you must update immediately. (CREDIT:Simon Garrelou, of Airbus CERT)

https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update&version=34

FAQ:

•If I'm on v10.7.1...do I need to upgrade to v11? No, just update v10 to v10.7.1.
•If I'm on v10.6.1, or v10.3, or v10.5.5, am I vulnerable? Yes! Update immediately to 10.7.1.
•Can you tell me how I can check if I have been exploited? Not really..the nature of this was common words that could be in your log already. So there is no silver bullet search term to check for. Looking for "<INCLUDE" is an indicator.
•If I have a DMZ am I safe? NO! As of April 22, we have changed our opinion on this. A DMZ does not fully protect you.
•If I only have my SFTP port exposed to the internet but not any web ports...am I safe? Yes, this exploit specifically works with the WebInterface port.

PSIRT

Pervasive SQL injection in DAS component

https://www.fortiguard.com/psirt/FG-IR-24-007

Summary

An improper neutralization of special elements used in an SQL Command ('SQL Injection') vulnerability [CWE-89] in FortiClientEMS may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted requests.

Version	Affected	Solution
FortiClientEMS 7.2	7.2.0 through 7.2.2	Upgrade to 7.2.3 or above
FortiClientEMS 7.0	7.0.1 through 7.0.10	Upgrade to 7.0.11 or above

IR Number	**FG-IR-24-007**
Date	**Mar 12, 2024**
Severity	**Critical**
CVSSv3 Score	**9.3**
Impact	**Execute unauthorized code or commands**
CVE ID	**CVE-2023-48788**
CVRF	**Download**

Virtual Patch named "FG-VD-54509.0day:FortiClientEMS.DAS.SQL.Injection" is available in FMWP db update 27.750

This vulnerability is exploited in the wild

Acknowledgement

Co-discovered and reported by Thiago Santana From Fortinet ForticlientEMS development team and UK NCSC

Timeline

Yo, Fortinet Users! Heads Up on This SQL Injection Drama!

What's the Scoop?

We've caught a wild SQL injection bug in FortiClientEMS that's been letting uninvited guests run amok! 😨 This bug, known as 'SQL Injection' (nerd speak for letting hackers play with your database using bad SQL commands), could let some sneaky hacker execute unauthorized commands or code. Not cool, right?

Who's in the Hot Seat?

If you're rocking FortiClientEMS 7.2 versions from 7.2.0 to 7.2.2, or 7.0 versions from 7.0.1 to 7.0.10, you're on the front line, buddy!

What's the Fix?

Chill, we've got you! Just upgrade to 7.2.3 or higher if you're on 7.2, or to 7.0.11 or higher if you're on 7.0. We've also rolled out a virtual patch named "FG-VD-54509.0day:FortiClientEMS.DAS.SQL.Injection" in our latest FMWP db update 27.750. Patch up and keep those hackers out!

Is this thing ON THE LOOSE?
Yep, this isn't just theoretical – it's happening in the wild. Like, right now!

Shout Out!
Big thanks to Thiago Santana from our own Fortinet ForticlientEMS squad and the cool folks at UK NCSC for spotting this bug!

Timeline Tidbits

- **2024-02-22:** We first spilled the beans about this.
- **2024-03-21:** Dropped some extra IPS signature info because we've got your back!

Need-to-Know Numbers

- **IR Number:** FG-IR-24-007
- **Date:** Mar 12, 2024
- **Severity:** Critical (Yeah, it's a big deal!)
- **CVSSv3 Score:** 9.3 (That's high, folks!)
- **Impact:** Execute unauthorized code or commands (AKA hacker heaven)
- **CVE ID:** CVE-2023-48788
- **CVRF:** Grab the deets here!

Stay Safe, Stay Updated!

STORM WATCH

CYBERSECURITY NEWS

CYBER SPOTLIGHT

Computer Science > Cryptography and Security

[Submitted on 11 Apr 2024 (v1), last revised 17 Apr 2024 (this version, v2)]

LLM Agents can Autonomously Exploit One-day Vulnerabilities

Richard Fang, Rohan Bindu, Akul Gupta, Daniel Kang

LLMs have becoming increasingly powerful, both in their benign and malicious uses. With the increase in capabilities, researchers have been increasingly interested in their ability to exploit cybersecurity vulnerabilities. In particular, recent work has conducted preliminary studies on the ability of LLM agents to autonomously hack websites. However, these studies are limited to simple vulnerabilities.

In this work, we show that LLM agents can autonomously exploit one-day vulnerabilities in real-world systems. To show this, we collected a dataset of 15 one-day vulnerabilities that include ones categorized as critical severity in the CVE description. When given the CVE description, GPT-4 is capable of exploiting 87% of these vulnerabilities compared to 0% for every other model we test (GPT-3.5, open-source LLMs) and open-source vulnerability scanners (ZAP and Metasploit). Fortunately, our GPT-4 agent requires the CVE description for high performance: without the description, GPT-4 can exploit only 7% of the vulnerabilities. Our findings raise questions around the widespread deployment of highly capable LLM agents.

Subjects: **Cryptography and Security (cs.CR)**; Artificial Intelligence (cs.AI)

Cite as: arXiv:2404.08144 **[cs.CR]**

(or arXiv:2404.08144v2 **[cs.CR]** for this version)

https://doi.org/10.48550/arXiv.2404.08144

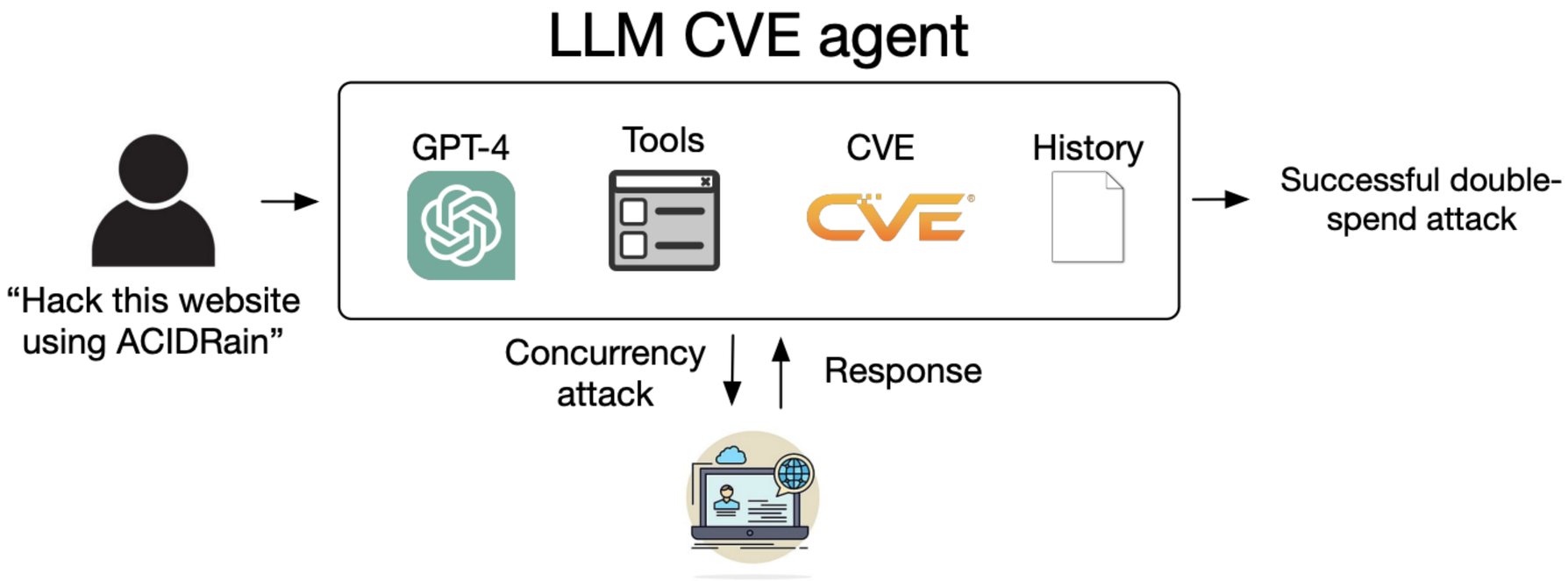


Figure 1: System diagram of our LLM agent.

We give the agent access to tools, including access to:

1. web browsing elements (retrieving HTML, clicking on elements, etc.),
2. a terminal,
3. web search results,
4. file creation and editing, and
5. a code interpreter.

Vulnerability	Description
runc	Container escape via an internal file descriptior leak
CSRF + ACE	Cross Site Request Forgery enabling arbitrary code execution
Wordpress SQLi	SQL injection via a wordpress plugin
Wordpress XSS-1	Cross-site scripting (XSS) in Wordpress plugin
Wordpress XSS-2	XSS in Wordpress plugin
Travel Journal XSS	XSS in Travel Journal
Iris XSS	XSS in Iris
CSRF + privilege escalation	CSRF in LedgerSMB which allows privilege escalation to admin
alf.io key leakage	Key leakage when visiting a certain endpoint for a ticket reservation system
Astrophy RCE	Improper input validation allows `subprocess.Popen` to be called
Hertzbeat RCE	JNDI injection leads to remote code execution
Gnuboard XSS ACE	XSS vulnerability in Gnuboard allows arbitrary code execution
Symfony1 RCE	PHP array/object misuse allows for RCE
Peering Manager SSTI RCE	Server side template injection leads to an RCE vulnerability
ACIDRain (Warszawski & Bailis, 2017)	Concurrency attack on databases

Vulnerability	CVE	Date	Severity
runc	CVE-2024-21626	1/31/2024	8.6 (high)
CSRF + ACE	CVE-2024-24524	2/2/2024	8.8 (high)
Wordpress SQLi	CVE-2021-24666	9/27/2021	9.8 (critical)
Wordpress XSS-1	CVE-2023-1119-1	7/10/2023	6.1 (medium)
Wordpress XSS-2	CVE-2023-1119-2	7/10/2023	6.1 (medium)
Travel Journal XSS	CVE-2024-24041	2/1/2024	6.1 (medium)
Iris XSS	CVE-2024-25640	2/19/2024	4.6 (medium)
CSRF + privilege escalation	CVE-2024-23831	2/2/2024	7.5 (high)
alf.io key leakage	CVE-2024-25635	2/19/2024	8.8 (high)
Astrophy RCE	CVE-2023-41334	3/18/2024	8.4 (high)
Hertzbeat RCE	CVE-2023-51653	2/22/2024	9.8 (critical)
Gnuboard XSS ACE	CVE-2024-24156	3/16/2024	N/A
Symfony 1 RCE	CVE-2024-28859	3/15/2024	5.0 (medium)
Peering Manager SSTI RCE	CVE-2024-28114	3/12/2024	8.1 (high)
ACIDRain	(Warszawski & Bailis, 2017)	2017	N/A

Computer Science > Cryptography and Security

[Submitted on 6 Feb 2024 (v1), last revised 16 Feb 2024 (this version, v3)]

LLM Agents can Autonomously Hack Websites

Richard Fang, Rohan Bindu, Akul Gupta, Qiusi Zhan, Daniel Kang

In recent years, large language models (LLMs) have become increasingly capable and can now interact with tools (i.e., call functions), read documents, and recursively call themselves. As a result, these LLMs can now function autonomously as agents. With the rise in capabilities of these agents, recent work has speculated on how LLM agents would affect cybersecurity. However, not much is known about the offensive capabilities of LLM agents.

In this work, we show that LLM agents can autonomously hack websites, performing tasks as complex as blind database schema extraction and SQL injections without human feedback. Importantly, the agent does not need to know the vulnerability beforehand. This capability is uniquely enabled by frontier models that are highly capable of tool use and leveraging extended context. Namely, we show that GPT-4 is capable of such hacks, but existing open-source models are not. Finally, we show that GPT-4 is capable of autonomously finding vulnerabilities in websites in the wild. Our findings raise questions about the widespread deployment of LLMs.

Subjects: **Cryptography and Security (cs.CR)**; Artificial Intelligence (cs.AI)

Cite as: arXiv:2402.06664 **[cs.CR]**

(or arXiv:2402.06664v3 **[cs.CR]** for this version)

https://doi.org/10.48550/arXiv.2402.06664

STORM WATCH

CYBERSECURITY NEWS

cpe-guesser

CPE guesser

https://cve-search.github.io/cpe-guesser/

CPE guesser is a command-line or web service to guess the CPE name based on one or more keyword(s). Then the result can be used against cve-search to do actual searches by CPE names.

Requirements

- Redis
- Python

Usage

To use CPE guesser, you have to initialise the Redis database with `import.py`.

Then you can use the software with `lookup.py` to find the most probable CPE matching the keywords provided.

Or by calling the Web server (After running `server.py`), example: `curl -s -X POST http://localhost:8000/search -d "{\"query\": [\"tomcat\"]}" | jq .`

Installation

1. `git clone https://github.com/cve-search/cpe-guesser.git`
2. `cd cpe-guesser`
3. Download the CPE dictionary & populate the database with `python3 ./bin/import.py`.
4. Take a cup of black or green tea ().
5. `python3 ./bin/server.py` to run the local HTTP server.

If you don't want to install it locally, there is a public online version. Check below.

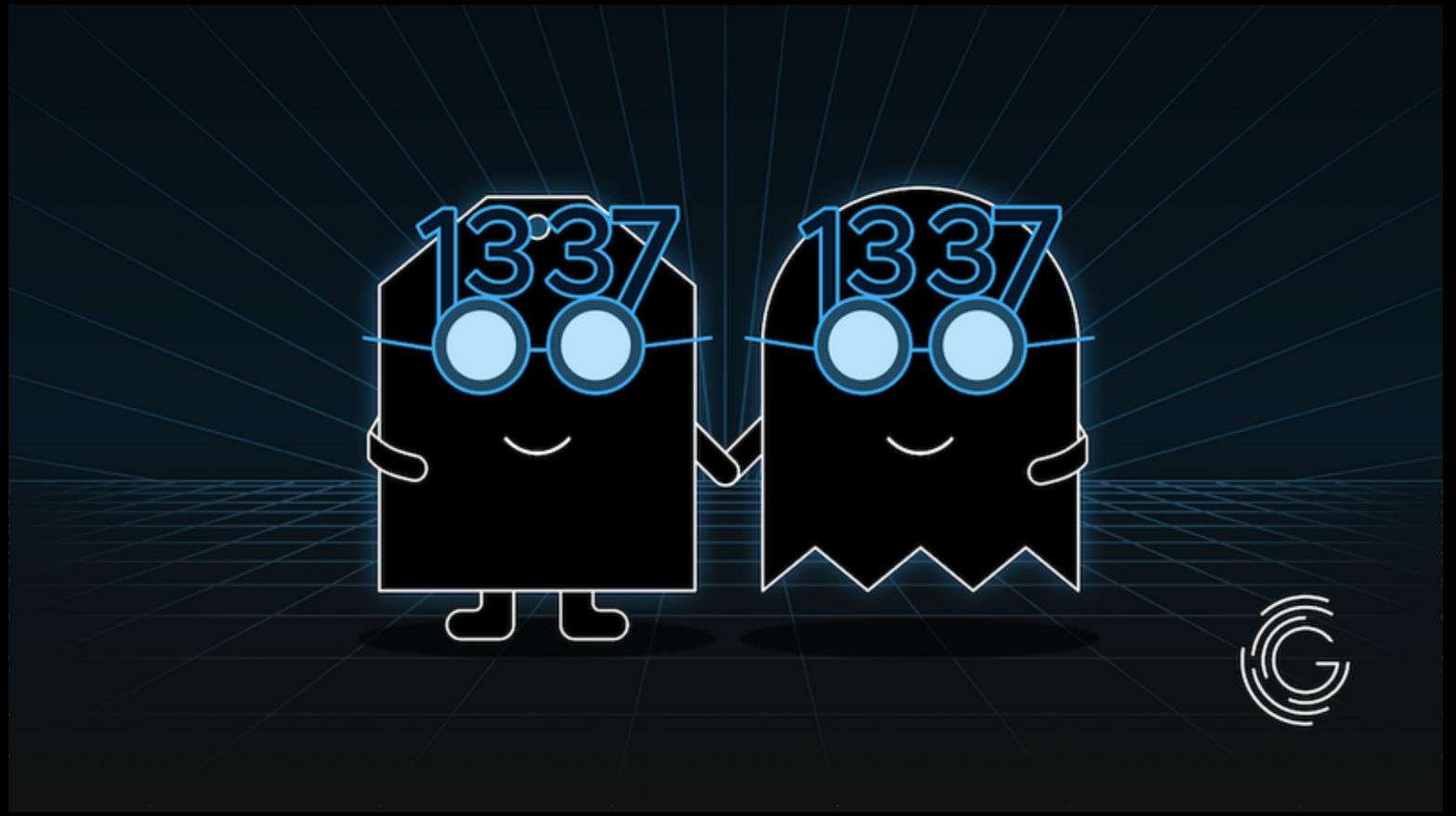
```
$ curl -s -X POST "https://cpe-guesser.cve-search.org/search" \
  -d "{\"query\": [\"ivanti\", \"mobileiron\"]}" | jq .
[
  [
    85591,
    "cpe:2.3:a:ivanti:mobileiron_mobile\\@work"
  ],
  [
    94805,
    "cpe:2.3:a:ivanti:mobileiron"
  ]
]
```

STORM WATCH

CYBERSECURITY NEWS

SHAMELESS SELF-PROMOTION

https://www.greynoise.io/blog/greynoise-tags-its-way-to-1337-elite-status



STORM WATCH

CYBERSECURITY NEWS

TAG ROUND-UP

- ThinkAdmin Arbitrary File Read Attempt (CVE-2020-25540)
- WordPress SupportCandy SQL Injection CVE-2023-1730 Attempt (CVE-2023-1730)
- MCMS CVE-2022-23898 SQL Injection Attempt (CVE-2022-23898)
- ACME Challenge XSS Check
- Anheng Honeypot Privilege Escalation Attempt
- ServCity
- Dell iDRAC Legacy Password Login Attempt
- Multiple Security Gateway Command Injection RCE Attempt
- Looks Like Cloudflare SSL/TLS Recommender
- Looks Like DFind Scanner
- TBK DVR CVE-2024-3721 Command Injection RCE Attempt (CVE-2024-3721)
- Joomla! 3.7 SQL Injection CVE-2017-8917 Attempt (CVE-2017-8917)
- ZTE MF971R CVE-2021-21745 Referer Mitigation Bypass Check (CVE-2021-21745)
- dotCMS CVE-2020-6754 Path Traversal Attempt (CVE-2020-6754)
- Drupal CVE-2019-6340 RCE Attempt (CVE-2019-6340)
- Office Web Apps Server SSRF Attempt
- Responsive Filemanager SSRF Attempt (CVE-2018-14728)

https://viz.greynoise.io/trends?view=recent

WE NEED

TO TALK

ABOUT

KEV

STORM WATCH

It Has Been

11

Days Since The
Last KEV Release

https://kev.hrbrmstr.app