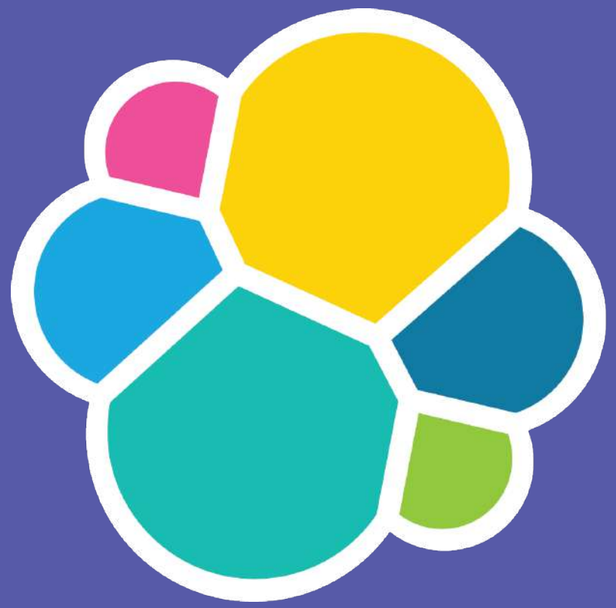
Security Tradeoffs in

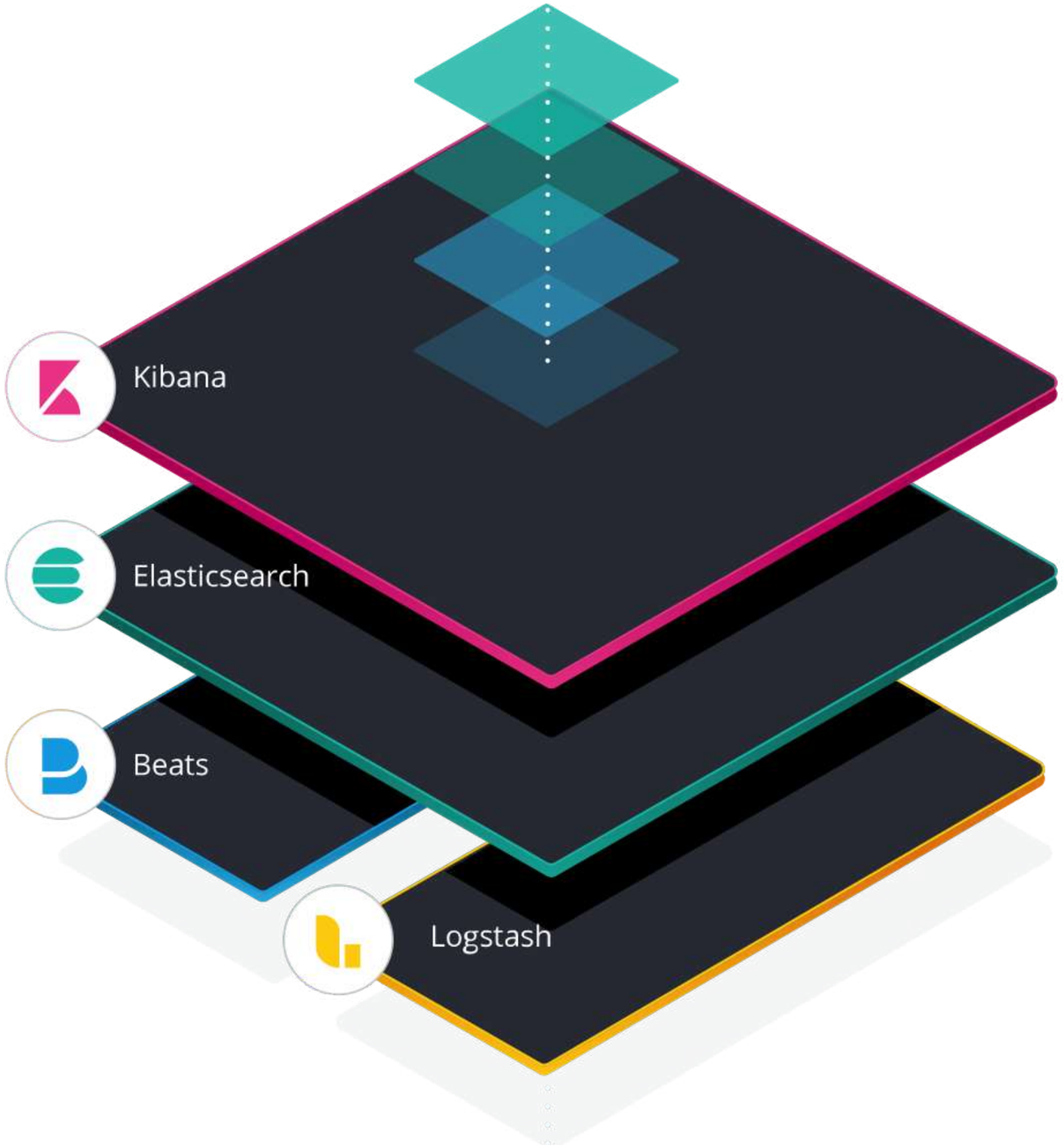
elasticsearch

Philipp Krenn @xeraa



elastic

Developer 🥑


Kibana
Elasticsearch
Beats
Logstash

Marcus Fulbright
@MarcusFulbright

Follow

Best argument for NoSQL: You can't have SQL injection attacks if you don't have SQL.

1:32 AM - 27 Oct 2017

8 Retweets **16** Likes

4 8 16

Did NoSQL improve security?

Thesis

Ease of use to grow, but...

BIND

to all Interfaces

Cluster

automatically

Production

vs development mode

https://github.com/elastic/elasticsearch/blob/7.7/server/src/main/java/org/elasticsearch/bootstrap/BootstrapChecks.java#L175-L188

```
/**
 * Tests if the checks should be enforced.
 *
 * @param boundTransportAddress the node network bindings
 * @param discoveryType the discovery type
 * @return {@code true} if the checks should be enforced
 */
static boolean enforceLimits(final BoundTransportAddress boundTransportAddress, final String discoveryType) {
    final Predicate<TransportAddress> isLoopbackAddress = t -> t.address().getAddress().isLoopbackAddress();
    final boolean bound =
            !(Arrays.stream(boundTransportAddress.boundAddresses()).allMatch(isLoopbackAddress) &&
            isLoopbackAddress.test(boundTransportAddress.publishAddress()));
    return bound && !"single-node".equals(discoveryType);
}
```

Bootstrap

Checks

elastic

- **Bootstrap Checks**
  - Heap size check
  - File descriptor check
  - Memory lock check
  - Maximum number of threads check
  - Max file size check
  - Maximum size virtual memory check
  - Maximum map count check
  - Client JVM check
  - Use serial collector check
  - System call filter check
  - OnError and OnOutOfMemoryError checks
  - Early-access check
  - G1GC check
  - All permission check
  - Discovery configuration check

Root

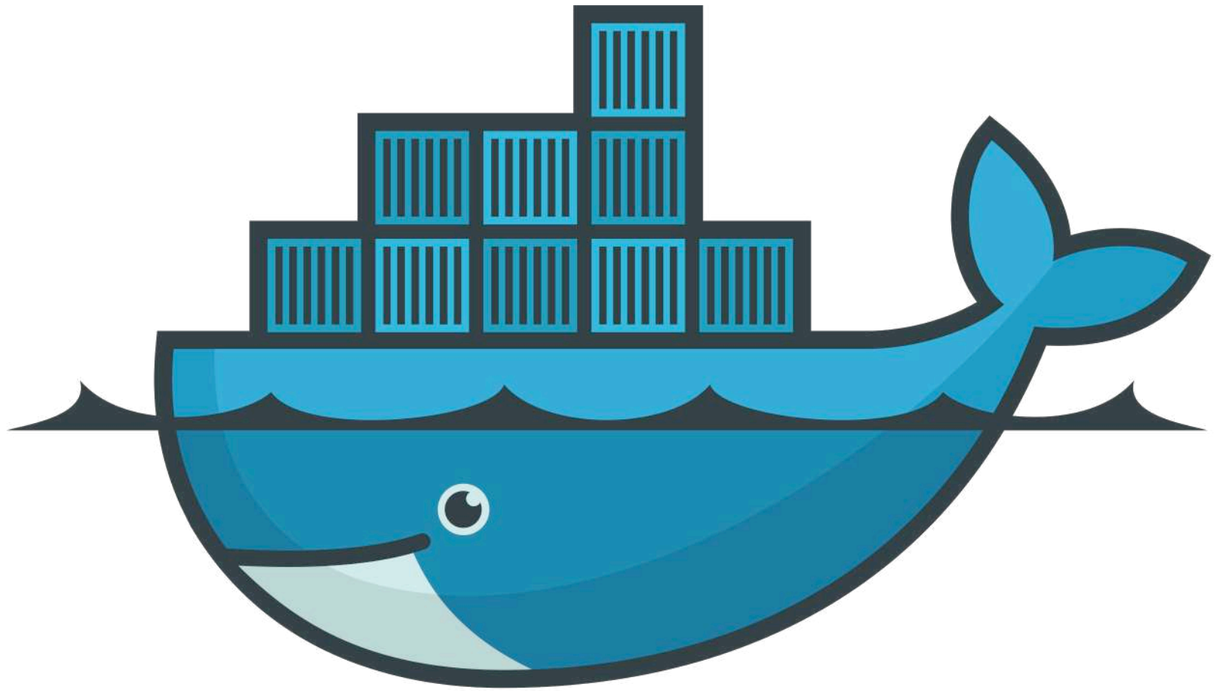
for Elasticsearch

https://github.com/elastic/elasticsearch/blob/7.7/server/src/main/java/org/elasticsearch/bootstrap/JNANatives.java#L165-L176

```
/** Returns true if user is root, false if not, or if we don't know */
static boolean definitelyRunningAsRoot() {
    if (Constants.WINDOWS) {
        return false; // don't know
    }
    try {
        return JNACLibrary.geteuid() == 0;
    } catch (UnsatisfiedLinkError e) {
        // this will have already been logged by Kernel32Library, no need to repeat it
        return false;
    }
}
```

https://github.com/elastic/elasticsearch/blob/7.7/server/src/main/java/org/elasticsearch/bootstrap/Bootstrap.java#L109-L112

```
// check if the user is running as root, and bail
if (Natives.definitelyRunningAsRoot()) {
    throw new RuntimeException("can not run elasticsearch as root");
}
```



docker

Levino commented on 26 Apr 2017

You should run the process as root. This is not increasing security but merely annoying.

👍 7 👎 18

https://github.com/elastic/elasticsearch-docker/issues/21#issuecomment-297439947

Scripting

with a general purpose language

"Why build a brand new language when there are already so many to choose from?"

https://www.elastic.co/blog/painless-a-new-scripting-language

Secure & performant

Removed Groovy, Python, JavaScript

in 6.0

Content-Type

guessing

```
curl 'http://localhost:9200/_search' -d'
{
    "query" : {
        "match_all" : {}
    }
}'
```

`text/plain` treated as safe

https://www.elastic.co/blog/strict-content-type-checking-for-elasticsearch-rest-requests

```
<html>
  <body>
    <script src="https://code.jquery.com/jquery-3.2.1.min.js"
            type="text/javascript"></script>
    <script type="text/javascript">
      $(function() {
        $.ajax({
          url: "http://localhost:9200/visitors/doc/",
          type:'POST',
          data: JSON.stringify({ browser: navigator.userAgent,
                                 date: new Date() }),
          contentType: 'text/plain'
        });
      });
    </script>
  </body>
</html>
```

Default

credentials

elastic/changeme

Removed in 6.0

How to set up?

TAR.GZ, DEB, RPM, MSI, Docker, Ansible, Helm, Operator,...

Env variable `ELASTIC_PASSWORD`

Clear-Text

credentials

`bin/elasticsearch-keystore`

Password-protected since 7.7, obfuscated before

TLS

certificates

bin/elasticsearch-certutil

Authentication

defaults

Free in 6.8 / 7.1 because K8s

https://www.elastic.co/blog/security-for-elasticsearch-is-now-free

On by default for everyone?

Next major version or later?

Mandatory for paid production setups

TOTAL RESULTS

15,356

TOP COUNTRIES

United States	3,968
China	2,908
France	1,023
Germany	721
Netherlands	632

TOP ORGANIZATIONS

Amazon.com	1,669
Hangzhou Alibaba Advertisin...	1,191
Microsoft Azure	675
OVH SAS	663
Digital Ocean	568

TOP OPERATING SYSTEMS

Linux 3.x	14
Windows 7 or 8	1

TOP PRODUCTS

Elastic	9,137
Elasticheney	118

Welcome to Badoo!

31.222.67.197
u98.badoo.com
Greysom Limited
Added on 2017-12-06 16:20:41 GMT
United Kingdom
Details

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 06 Dec 2017 16:20:41 GMT
Content-Type: text/html
Content-Length: 344
Last-Modified: Wed, 28 Sep 2016 15:37:33 GMT
Connection: keep-alive
ETag: "57ebe3bd-158"
Expires: Thu, 06 Dec 2018 16:20:41 GMT
Cache-Control: max-age=31536000
Cache-Control: no...
```

广发证券（香港）预约开户

59.41.16.181
China Telecom Guangdong
Added on 2017-12-06 16:18:52 GMT
China, Guangzhou
Details

```
HTTP/1.1 200 OK
Vary: Accept-Encoding
Last-Modified: Mon, 13 Nov 2017 06:06:57 GMT
Content-Length: 775
Cache-Control: max-age=0
Content-Type: text/html; charset=utf-8
ETag: W/"307-15fb3fce7e8"
X-Response-Time: 6ms
Date: Wed, 06 Dec 2017 16:52:09 GMT
Connection: keep-alive
```

5.79.76.116

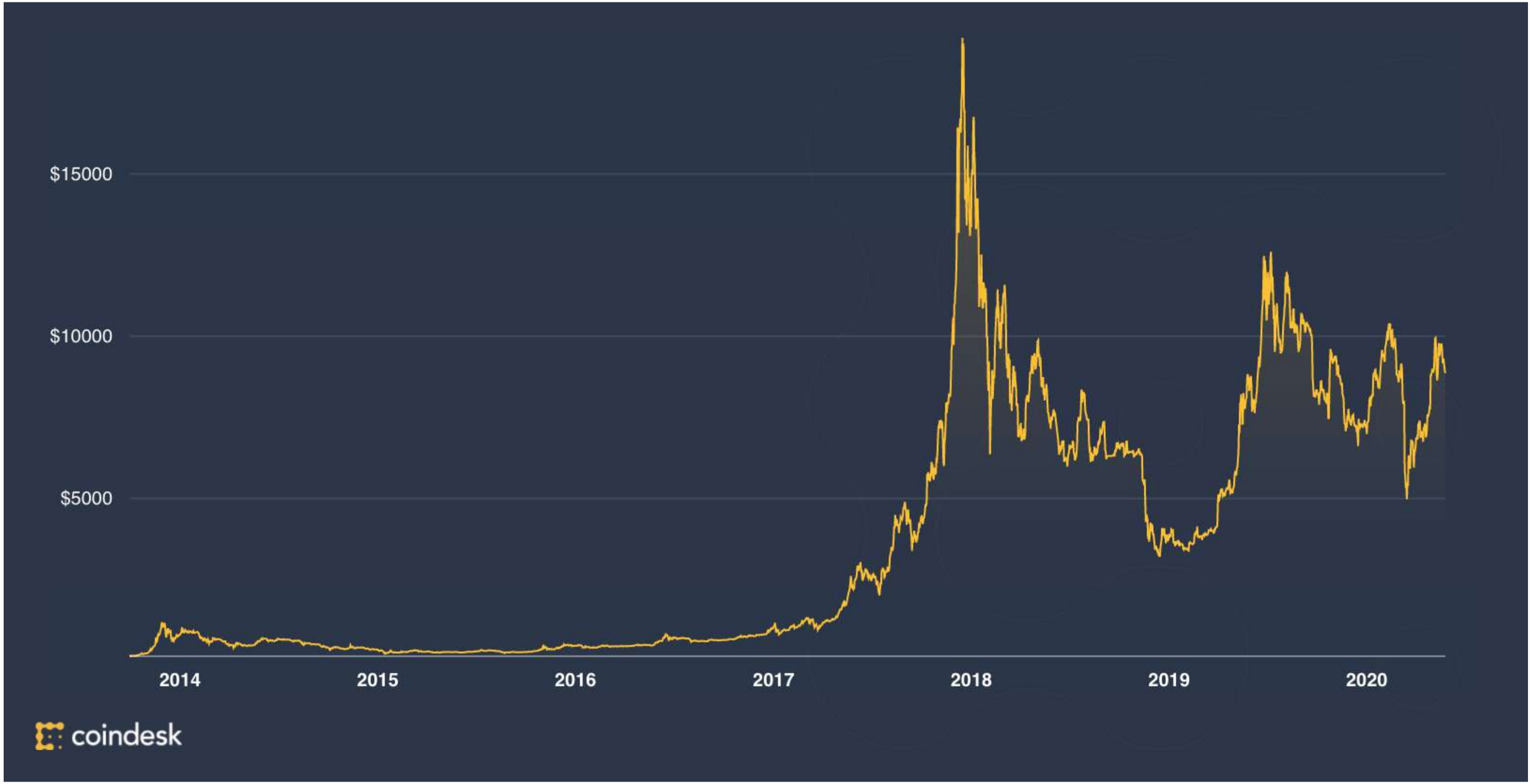
LeaseWeb Netherlands B.V.
Added on 2017-12-06 16:17:23 GMT
Netherlands
Details

4.0 kB | 1 Nodes

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 341
```

```
$ curl -XGET 'http://67.205.153.88:9200/_cat/indices'
yellow open goal12       5 1 9397 0   27mb   27mb
yellow open please_read 5 1    1 0  4.9kb  4.9kb
yellow open un-webhose  5 1 2294 1 25.4mb 25.4mb
yellow open goal11       5 1 4828 0 13.3mb 13.3mb
```

```
$ curl -XGET 'http://67.205.153.88:9200/please_read/_search?pretty'
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "failed" : 0
  },
  "hits" : {
    "total" : 1,
    "max_score" : 1.0,
    "hits" : [ {
      "_index" : "please_read",
      "_type" : "info",
      "_id" : "AVm3qmXeus_FduwRD54v",
      "_score" : 1.0,
      "_source" : {
        "Info" : "Your DB is Backed up at our servers, to restore send 0.5 BTC
                  to the Bitcoin Address then send an email with your server ip",
        "Bitcoin Address" : "12JNfaS2Gzic2vqzGMvDEo38MQSX1kDQrx",
        "Email" : "elasticsearch@mail2tor.com"
      }
    } ]
  }
}
```


$15000
$10000
$5000
2014
2015
2016
2017
2018
2019
2020
coindesk

On 03 Feb 14:12, reports@reports.cert-bund.de wrote:

> Dear Sir or Madam,
>
> Elasticsearch is a popular search engine based on Apache Lucene, often used with web applications.
>
> If an Elasticsearch server is openly accessible from the Internet and not protected by any forms of authentification, anyone who can connect to the server has unrestricted access to the data stored with it. This allows attackers to modify or delete any data or potentially steal sensitive information. In addition, prior to versions 1.2.x an attacker can use dynamic scripting to perform arbitrary code execution on the machine that Elasticsearch is hosted on.
>
> Affected systems on your network:
>
> Format: ASN | IP | Timestamp (UTC) | Elasticsearch version | Instance name
> 24940 | [redacted].176 | 2018-02-02 04:14:47 | 6.2.0 | docker-test-node-1

Thesis

...security for critical workloads

Conclusion

Bind & cluster

Bootstrap checks & root

Scripting

Content-type

Default & clear-text credentials

TLS

Authentication

Security Tradeoffs in

elasticsearch

Philipp Krenn @xeraa