D4Science Infrastructure - Incident #482

GARR-CERT-16H1208 Unrestricted elasticsearch server access on node13.p.d4science.research-infrastructures.eu

Aug 12, 2015 11:32 AM - Andrea Dell'Amico

Status:	Closed	**Start date:**	Aug 12, 2015
Priority:	Immediate	**Due date:**	
Assignee:	_InfraScience Systems Engineer	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	UnSprintable		
Infrastructure:	Production		

Description

GARR-CERT reports that node13.p.d4science.research-infrastructures.eu has an elasticsearch instance main port open to the world:

```
############################################################
Incident Number: GARR-CERT-16H1208
############################################################

Salve,

sono un membro del GARR-CERT (www.cert.garr.it), il Computer
Security Incident Response Team della rete GARR (www.garr.it),
la rete Accademica e della Ricerca in Italia.

Abbiamo ricevuto un report in base al quale il software Elasticsearch
in funzione sull'host node13.p.d4science.research-infrastructures.eu
(146.48.122.236), risulta raggiungibile ed interrogabile da qualsiasi
nodo in internet.

timestamp,ip,proto,port,hostname,tag,version,naics,sic,ok,name,cluster_name,status,build_hash,buil
d_timestamp,build_snapshot,lucene_version,tagline
2015-08-02 06:48:25,146.48.122.236,tcp,9200,node13.p.d4science.research-infrastructures.eu,elastic
search,1.5.0,0,0,,Amphibion,es-cluster--d4science.research-infrastru,200,544816042d40151d3ce4ba4f9
5399d7860dc2e92,2015-03-23T14:30:58Z,false,4.10.4,You Know, for Search


Elasticsearch non prevede alcuna autenticazione o limitazione di accesso
ai dati, e' quindi possible che chiunque possa ottenere un controllo
completo del servizio e attuare abusi.

Vi suggeriamo di configurare delle restrizioni
in modo da controllare l'accesso al server.


Riferimenti:

https://www.elastic.co/products/elasticsearch

https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Elasticsearch

https://www.tenable.com/plugins/index.php?view=single&id=76572
http://bouk.co/blog/elasticsearch-rce/

http://stackoverflow.com/questions/4960298/how-to-secure-an-internet-facing-elastic-search-impleme
ntation-in-a-shared-hosti
https://github.com/sonian/elasticsearch-jetty

https://github.com/floragunncom/search-guard
http://stackoverflow.com/questions/31366406/search-guard-not-integrating-with-elasticsearch

Cordiali saluti,
```

```
GARR-CERT staff

~-------------------------------------------------------------------
Andrea Pinzani         G A R R - C E R T       tel. +39 055 4572723
Italian Academic and Research Network            http://www.garr.it
Computer Security Incident Response Team    http://www.cert.garr.it
PGP key: http://www.cert.garr.it/PGP/keys.php3#ap
~-------------------------------------------------------------------
```

History

#1 - Aug 12, 2015 11:37 AM - Andrea Dell'Amico

- Status changed from New to In Progress

- % Done changed from 0 to 90

I see that it's an index service that runs on a tomcat instance listening on port 8080. The webapp includes the elasticsearch libraries.

I'm leaving the port 8080 open to the world, while I'm closing the 9200 port to everybody but the ISTI and ISTI-Eduroam networks.
Let me know if it's correct. The running iptables rules:

```
    0     0 ACCEPT     tcp  --  *      *       146.48.122.236       0.0.0.0/0           state NEW tcp dpt:920
0
    0     0 ACCEPT     tcp  --  *      *       146.48.80.0/21       0.0.0.0/0           state NEW tcp dpt:920
0
    0     0 ACCEPT     tcp  --  *      *       146.48.122.0/23      0.0.0.0/0           state NEW tcp dpt:920
0
    0     0 ACCEPT     tcp  --  *      *       146.48.51.0/24       0.0.0.0/0           state NEW tcp dpt:920
0
    0     0 ACCEPT     tcp  --  *      *       146.48.106.0/23      0.0.0.0/0           state NEW tcp dpt:920
0
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:920
0 reject-with icmp-host-prohibited
```

#2 - Aug 13, 2015 03:45 PM - Tommaso Piccioli

- Status changed from In Progress to Closed

- % Done changed from 90 to 100

##
Incident Number: GARR-CERT-16H1208 CLOSED
##

Salve,

il ticket in oggetto e' stato chiuso.
Grazie per la collaborazione.

Cordiali saluti,
GARR-CERT staff