Advanced Notification of Cyber Threats against Publicly Accessible Databases Engines

Security Advisory	ADV-19-07	**Criticality**	High	○○○●
Advisory Released On	13 March 2019			

Impact

Misconfiguring database engines could allow leakage of highly sensitive information / data belonging to entities.

Solution

Adhere the advices written under the recommendations section.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a critical risk in misconfiguring databases engines or application servers. Misconfiguration of database engines can result in no protection to highly sensitive information, leakage of data, and ransacking of private data. Entities should prohibit public access to the databases, as it reverses the purpose of high security measures that are engaged by entities to secure their various services, such as websites and applications. Misconfiguring database engines to allow public access will result in no protection, even if the entity has secured their other services with a high security standard.

Details

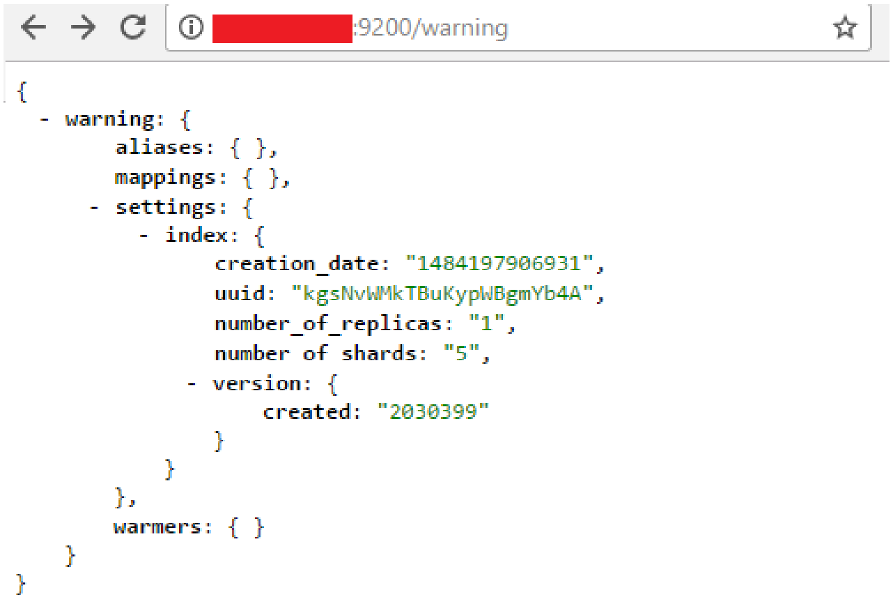
Database engines are the back-end technology for application servers, in which the application data is stored and managed. The database clusters could contain extremely confidential information related to an entity, their partnered constituents, and their clients.

Protecting the confidentiality of data is a priority for entities, thereby there are high security measures implemented in their services, such as (HTTPS, IDS, Firewall, and etc.). The database cluster for services is managed by database engines. The misconfiguration of database engines could result in no protection, as it avoids the implemented security measures, and leading to leakage and ransacking of highly sensitive information.

Attackers may attempt to ransack misconfigured database engines to attain data belonging to entities. To secure the database further, the deployment of database engines, such as Elasticsearch, MongoDB, and other engines must be configured properly.

In cases where there is misconfiguration that allow for public access in database, the data would be easily accessible via internet.

Example of direct access to misconfigured database via web browser:



[redacted]:9200/warning

```
{
 - warning: {
       aliases: { },
       mappings: { },
     - settings: {
         - index: {
               creation_date: "1484197906931",
               uuid: "kgsNvWMkTBuKypWBgmYb4A",
               number_of_replicas: "1",
               number of shards: "5",
             - version: {
                   created: "2030399"
               }
           }
       },
       warmers: { }
   }
}
```

Recommendations

To avoid ransack of database engines, entities are recommended with the following:

- Implement security check and hardening on database engines to ensure that the databases/ servers are not accidentally exposed to internet.
- Access to database servers should restricted to only authorized application/ users and allowed only via access controlled internal network
- Change the default ports used by the database engines
- The hosting of services such as mail, website, applications, and databases that contain data of UAE citizens and residents should be hosted in U.A.E.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel	(+971) 4 777 4003
Fax	(+971) 4 777 4100
Email	info[at]aeCERT.ae
Instagram	@TheUAETRA
Twitter	@TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae