

Bash 漏洞原理及利用

漏洞原理

Bash 漏洞原理如下：

- 漏洞成因：在 Bash 4.2 之前版本中，当环境变量名包含特殊字符（如分号、反引号等）时，会导致命令解析出现异常，从而引发漏洞。
- 利用条件：攻击者需要具备对目标系统的环境变量进行操控的能力（如 RHEL 4 之前版本，或者通过某些配置实现）。攻击者需要知道目标系统使用的是 Bash 4.2 之前版本。
- 攻击原理：攻击者通过设置特殊的环境变量，使得在调用 Bash 时，解析器会错误地执行攻击者指定的命令，而不是预期的系统命令。
- 攻击效果：攻击者可以在目标系统上执行任意命令，实现提权或系统控制。

攻击步骤如下：

- 攻击者构造恶意的环境变量并执行命令。

```
[root@localhost ~]# env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
(vulnerable@localhost ~) #
```

- 攻击者利用漏洞在目标系统上执行命令。

```
[root@localhost ~]# yum update bash -y
```

- 攻击者再次构造恶意的环境变量并执行命令。

```
[root@localhost ~]# env x='() { :; }; echo vulnerable' bash -c "echo this is a test"
this is a test
```

- 攻击者通过设置特殊的环境变量，使得在调用 Bash 时，解析器会错误地执行攻击者指定的命令，而不是预期的系统命令。

```
[root@localhost ~]# grep -l -z '^[^)]=( ) {' /proc/[1-9]*/environ | cut -d/ -f3
```

Reference

- <https://rhn.redhat.com/errata/RHSA-2014-1293.html>
 - <https://access.redhat.com/articles/1200223////>
-

Revision #1

Created 7 June 2022 02:33:17 by artop0420

Updated 24 December 2023 00:40:03 by artop0420