NewStart CGSL V3.02.30.P3.F5版本

(Glibc堆缓冲区溢出漏洞CVE-2015-0235修复版本)发布说明

**CGSL项目组 2015-02-09**

# 版本获取方式

请通过我们的售后服务联系方式联系获取。

# 版本文件说明

CGSL V3.02.30.P3.F5版本(Glibc堆缓冲区溢出漏洞CVE-2015-0235修复版本)包括以下内容：

|  |  |  |
| --- | --- | --- |
| **文件类型** | **存放路径** | **说明** |
| **64位版本补丁程序** | /64位/glibc-2.5-123.el5\_11.1.x86\_64.rpm  /64位/glibc-devel-2.5-123.el5\_11.1.x86\_64.rpm  /64位/glibc-common-2.5-123.el5\_11.1.x86\_64.rpm  /64位/glibc-headers-2.5-123.el5\_11.1.x86\_64.rpm  /64位/glibc-2.5-123.el5\_11.1.i686.rpm  /64位/glibc-devel-2.5-123.el5\_11.1.i386.rpm  /64位/nscd-2.5-123.el5\_11.1.x86\_64.rpm | 适用版本(64位系统):  **V3.02系列所有版本** |
| **32位版本补丁程序** | /32位/glibc-2.5-123.el5\_11.1.i686.rpm  /32位/glibc-devel-2.5-123.el5\_11.1.i386.rpm  /32位/glibc-common-2.5-123.el5\_11.1.i386.rpm  /32位/glibc-headers-2.5-123.el5\_11.1.i386.rpm  /32位/nscd-2.5-123.el5\_11.1.i386.rpm | 适用版本(32位系统):  **V3.02系列所有版本** |
| **版本说明文档** | /NewStart CGS Linux V3.02.30.P3.F5版本信息说明.doc |  |

# 版本更新说明

**CGSL V3.02.30.P3.F5版本主要针对Glibc堆缓冲区溢出漏洞CVE-2015-0235(最新公布)提供修复补丁。**

Glibc 2.18之前版本中，\_\_nss\_hostname\_digits\_dots()函数存在堆缓冲区溢出漏洞，gethostbyname()及gethostbyname2()这两个glibc函数调用时会用到该函数。远程攻击者可通过glibc提供的接口编写恶意代码，利用此漏洞以当前用户权限执行任意代码，此漏洞对系统安全威胁较大，建议尽快修复。

CGSL当前各版本均受此漏洞影响。可通过部署补丁修复此漏洞，防止相应攻击的发生。

# 补丁程序的使用方法

1. 安装系统升级补丁程序前，请使用如下命令确认当前系统版本是否是在补丁适用范围内的版本，示例如下：

**#cat /etc/klinux-release**

**TAG\_CGS\_MAIN\_V3\_02\_20**

1. 请使用下面命令确认当前系统架构：

**#uname -ar**

如结果中有x86\_64的字段，则为64位系统，否则为32位系统。

1. 创建新目录，将本补丁所包含的所有rpm包拷贝到该目录中，并进入此目录。示例如下：

**#mkdir /tmp/glibc-patch**

**#cp glibc\*.rpm nscd\*.rpm /tmp/glibc-patch**

**#cd /tmp/glibc-patch**

1. 请确保当前用户具有root权限，然后执行如下命令升级原有的glibc组件：

**#rpm -Uvh \*.rpm**

1. 执行如下命令确认补丁包是否部署成功，如果相应的rpm包的版本号都已经更新为补丁中包含的rpm包的版本，则部署成功。示例如下：

32位系统：

**#rpm -qa | grep glibc**

**glibc-headers-2.5-123.el5\_11.1.i386**

**glibc-2.5-123.el5\_11.1.i686**

**glibc-devel-2.5-123.el5\_11.1.i386**

**glibc-common-2.5-123.el5\_11.1.i386**

**#rpm –qa|grep nscd**

**nscd-2.5-123.el5\_11.1.i386**

64位系统：

**#rpm -qa | grep glibc**

**glibc-headers-2.5-123.el5\_11.1.x86\_64**

**glibc-2.5-123.el5\_11.1.x86\_64**

**glibc-devel-2.5-123.el5\_11.1.x86\_64**

**glibc-2.5-123.el5\_11.1.x86\_64**

**glibc-devel-2.5-123.el5\_11.1.x86\_64**

**glibc-common-2.5-123.el5\_11.1.x86\_64**

**#rpm –qa|grep nscd**

**nscd-2.5-123.el5\_11.1.x86\_64**

1. 在确认补丁升级成功之后，按照下列方法执行测试代码，确认漏洞是否被修复。执行如下命令：

测试代码如下：



编译代码：

**#gcc ghost.c -o t**

然后运行：

**#./t**

**not vulnerable**

完成上述操作，如果执行结果打印vulnerable代表有漏洞，打印not vulnerable代表没有漏洞。

1. 确认漏洞修复后，**重启系统**，补丁部署完成。