

Linux Kernel 2.6 の udev の脆弱性に関する検証レポート

2009/4/21

NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Linux Kernel 2.6 以降で導入されている動的にデバイスファイルを作成する機能を実現する udev に脆弱性が存在することが発見されました。

この脆弱性により、ローカル環境において、一般ユーザに udev の脆弱性を利用した攻撃コードを実行され、管理者権限を奪取される恐れがあります。

想定される被害としては、管理者権限での情報取得、改ざんが考えられます。

今回、udev の脆弱性 (CVE-2009-1185) の再現性について検証を行いました。

【影響を受けるとされているシステム】

Linux Kernel 2.6 を利用しているシステム

【対策案】

現在使用中のディストリビューションの udev をアップデートすることが推奨されます。

Redhat

<https://rhn.redhat.com/errata/RHSA-2009-0427.html>

Debian

<http://www.debian.org/security/2009/dsa-1772>

SUSE

http://www.novell.com/linux/security/advisories/2009_20_udev.html

Ubuntu

<http://www.ubuntu.com/usn/usn-758-1>

Gentoo

<http://www.gentoo.org/security/en/glsa/glsa-200904-18.xml>

rPath

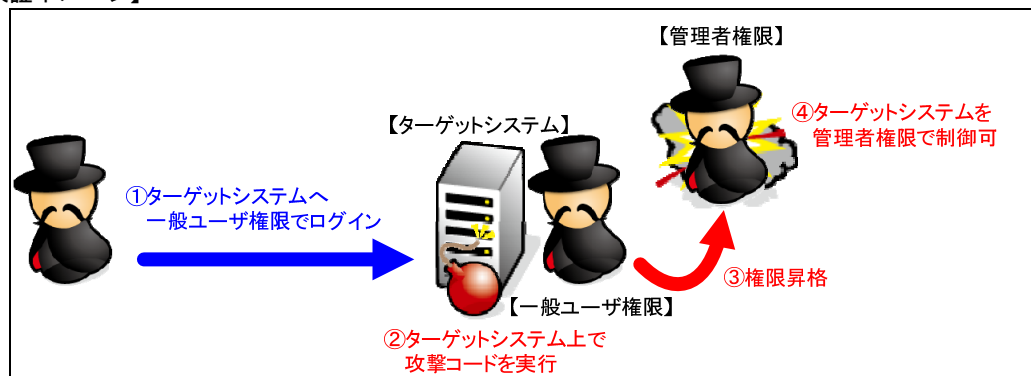
<https://issues.rpath.com/browse/RPL-3016>

【参考サイト】

CVE-2009-1185

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185>

【検証イメージ】



【検証ターゲットシステム】

Red Hat Enterprise Linux Server release 5
 Linux Kernel 2.6.18-8.el5
 udev-095-14.5.el5

【検証概要】

ターゲットシステムに一般ユーザでログインし、udev の脆弱性を利用した攻撃コードを実行することで、権限昇格させます。

これにより、ローカルからターゲットシステムを管理者権限で操作可能となります。

* この脆弱性は、ターゲットシステムに一般ユーザでログインできることが前提です。

【検証結果】

下図の赤線で囲まれている部分に示すように、ターゲットコンピュータに一般ユーザでログインしている情報を表しております。

黄色線で囲まれている部分は、攻撃コード実行後、ターゲットシステムにおいて、管理者権限「uid=0(root)」に昇格している情報を表しております。

```

ターゲットシステムの管理者権限の奪取に成功した画面

[test@localhost ~]$ id
uid=500(test) gid=500(test) 所属グループ=500(test) context=root:system_r:unconfined_t:SystemLow-SystemHigh
[test@localhost ~]$
[test@localhost ~]$ cat /proc/net/netlink
sk      Eth Pid  Groups  Rmem  Wmem  Dump  Locks
cfe0000 0 0 00000000 0 0 00000000 2
c12ed600 0 2199 00000111 0 0 00000000 2
cfe8a400 6 0 00000000 0 0 00000000 2
c12fd000 7 2497 00000001 0 0 00000000 2
c12f5a00 7 1884 00000001 0 0 00000000 2
cfe00a00 7 0 00000000 0 0 00000000 2
c12fae00 9 1739 00000000 0 0 00000000 2
cfcf1200 9 0 00000000 0 0 00000000 2
cfece8e00 10 0 00000000 0 0 00000000 2
cfe9fe00 11 0 00000000 0 0 00000000 2
c12f8a00 12 0 00000000 0 0 00000000 2
cfe0dc00 15 0 00000000 0 0 00000000 2
cfd94e00 15 390 ffffffff 0 0 00000000 2
cfe9fc00 16 0 00000000 0 0 00000000 2
cf284800 18 0 00000000 0 0 00000000 2
[test@localhost ~]$
[test@localhost ~]$ sh kernel_local.sh 390
suid.c: In function 'main':
suid.c:3: 警告: incompatible implicit declaration of built-in function 'execel'
sh-3.1# id
uid=0(root) gid=0(root) 所属グループ=500(test) context=root:system_r:unconfined_t:SystemLow-SystemHigh
sh-3.1#
  
```

【対策案】

現在使用中のディストリビューションの udev をアップデートすることが推奨されます。

Redhat

<https://rhn.redhat.com/errata/RHSA-2009-0427.html>

Debian

<http://www.debian.org/security/2009/dsa-1772>

SUSE

http://www.novell.com/linux/security/advisories/2009_20_udev.html

Ubuntu

<http://www.ubuntu.com/usn/usn-758-1>

Gentoo

<http://www.gentoo.org/security/en/glsa/glsa-200904-18.xml>

rPath

<https://issues.rpath.com/browse/RPL-3016>



NTTデータ・セキュリティ株式会社

【参考サイト】

CVE-2009-1185

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185>

* 各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ・セキュリティ株式会社

営業企画部

TEL:03-5425-1954

<http://www.nttdata-sec.co.jp/>