Обновления безопасности и методические указания Astra Linux Special Edition 1.5

Всё программное обеспечение, разработанное с использованием обновлений для дисков со средствами разработки, будет корректно функционировать только в среде ОС Astra Linux с установленными соответствующими обновлениями безопасности.

Как узнать версию установленного обновления Astra Linux SE?

Методические указания не являются кумулятивным обновлением безопасности. При выполнении методических указаний автоматическая установка обновлений безопасности не осуществляется, и обновления безопасности должны быть установлены отдельно.

БЮЛЛЕТЕНЬ № 20190719SE15MD

Методические указания по нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" (версия 1.5) в информационных системах.

В целях предотвращения эксплуатации уязвимостей BDU:2019-02313, BDU:2019-02628, BDU:2019-02609, BDU:2019-02629, позволяющим нарушителю вызвать отказ в обслуживании, рекомендуется выполнить обновление пакетов в соответствии с инструкцией, приведенной ниже.

Пакет	Идентификатор уязвимости
libflycore	BDU:2019-02609
goldendict	BDU:2019-02639, BDU:2019-02640
gnupg	BDU:2019-02629
linux-astra-modules	BDU:2019-02300

Загрузить архив по ссылке:

Скачать

Архив подписан усиленной квалифицированной электронной подписью АО "НПО РусБИТех" с использованием ключевого комплекта, выданного удостоверяющим центром Министерства Обороны Российской Федерации (Скачать).
Для проверки подписи необходимо добавить в локальное хранилище сертификаты головного удостоверяющего центра и списки отозванных сертификатов, размещенные на сайте: https://structure.mil.ru/structure/UC/certificate.htm

Распаковать архив:

```
tar xzvf 20190719.tar.gz
```

Перейти в директорию и установить пакеты:

```
cd 20190719

sudo dpkg -i *.deb
```

Вполнить команду для завершения установки пакетов:

```
sudo apt -f install
```

При этом если доступен диск со средствами разработки то будут восстановлены зависимости пакета для libflycore-dev, если диск со средствами разработки недоступен то этот пакет будет удалён.

В целях предотвращения эксплуатации уязвимостей, позволяющим нарушителю вызвать отказ в обслуживании, рекомендуется снять бит исполнения для непривилегированных пользователей со следующих утилит:

Имя файла	Пакет	Идентификатор уязвимости
/usr/bin/signtool	libnss3-tools	BDU:2019-02611
/usr/bin/unixcmd	vde2	BDU:2019-02612
/usr/bin/peekfd	psmisc	BDU:2019-02613
/usr/bin/makeinfo	texinfo	BDU:2019-02614
/usr/bin/nettle-hash	nettle-bin	BDU:2019-02615
/usr/bin/xkbevd	x11-xkb-utils	BDU:2019-02616
/usr/bin/genrb	icu-devtools	BDU:2019-02617
/usr/bin/dvipos	texlive-extra-utils	BDU:2019-02618
/usr/bin/pdftohtml	pdftohtml	BDU:2019-02621
/usr/bin/pdftops	poppler-utils	BDU:2019-02622
/usr/bin/vde_l3	vde2	BDU:2019-02623
/usr/bin/roarfilt	roarclients	BDU:2019-02624
/usr/bin/umax_pp	sane-utils	BDU:2019-02625
/usr/bin/fdtdump	device-tree-compiler	BDU:2019-02626
/usr/bin/faad	faad	BDU:2019-02627
/usr/bin/a2p	perl	BDU:2019-02628
/usr/bin/gtbl	groff-base	BDU:2019-02630
/usr/bin/infotocap	ncurses-bin	BDU:2019-02631, BDU:2019-02632
/usr/bin/workmanir	libirman-dev	BDU:2019-02634
/usr/bin/ppdhtml	cups-ppdc	BDU:2019-02635
/usr/bin/glxdemo	mesa-utils	BDU:2019-02636
/usr/bin/ppdpo	cups-ppdc	BDU:2019-02637
/usr/bin/fontlint	fontforge	BDU:2019-02638

Для удобства снятия бита исполнения, был подготовлен скрипт:

```
#!/bin/bash

files='signtool unixcmd peekfd makeinfo nettle-hash xkbevd
genrb dvipos pdftohtml pdftops vde_l3 roarfilt umax_pp
fdtdump faad a2p gtbl infotocap workmanir ppdhtml
glxdemo ppdpo fontlint'

for file in $files; do
    chmod -f -x /usr/bin/${file} && chmod u+x /usr/bin/${file}
done
```

Скачать script.sh

Сделать скрипт исполняемым:

```
chmod +x script.sh
```

Выполнить:

```
sudo ./script.sh
```

БЮЛЛЕТЕНЬ № 20190712SE15MD

Методические указания по нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" (версия 1.5) в информационных системах.

> Методические указания не являются кумулятивным обновлением безопасности. При выполнении методических указаний автоматическая установка обновлений безопасности не осуществляется, и обновления безопасности должны быть установлены отдельно.

Методика безопасности, нейтрализующая угрозу эксплуатации уязвимости BDU:2019-02442

Уязвимость компонента оконного менеджера fly-wm связанная с ошибками в алгоритме пересчета разрешения при изменения размера окна, позволяющая нарушителю получить доступ к конфиденциальным данным http://bdu.fstec.ru/vul/2019-02442

Для предотвращения эксплуатации указанной уязвимости необходимо выполнить обновление указанного пакета в соответствии с инструкцией, приведенной ниже.

> **Внимание**
>
> Обновление пакетов необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы с высоким уровнем целостности.
> На время установки обновления необходимо снять запрет на установку бита исполнения в политиках безопасности.

1.Загрузить архив по ссылке:

Ссылка

2.Проверить соответствие контрольной суммы, выполнив команду:

```
gostsum fly-wm-se15.tar.gz
```

```
f7fc6de81ee8716b03d3888467619ef960da3210dc01e7faee69a27c26a8ea22 fly-wm-se15.tar.gz
```

> Архив подписан усиленной квалифицированной электронной подписью АО "НПО РусБИТех" с использованием ключевого комплекта, выданного удостоверяющим центром Министерства Обороны Российской Федерации (Скачать).
> Для проверки подписи необходимо добавить в локальное хранилище сертификаты головного удостоверяющего центра и списки отозванных сертификатов, размещенные на сайте: https://structure.mil.ru/structure/UC/certificate.htm

3. Распаковать архив, выполнив:

```
tar xzf fly-wm-se15.tar.gz
```

4. Перейти в распакованную директорию fly-wm

```
cd fly-wm
```

5. Выполнить установку:

```
sudo dpkg -i *.deb
```

Внимание

Обновление пакетов необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы с высоким уровнем целостности.
На время установки обновления необходимо снять запрет на установку бита исполнения в политиках безопасности.

БЮЛЛЕТЕНЬ № 20190605SE15MD

Методические указания по нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" (версия 1.5) в информационных системах.

Методические указания не являются кумулятивным обновлением безопасности. При выполнении методических указаний автоматическая установка обновлений безопасности не осуществляется, и обновления безопасности должны быть установлены отдельно.

В целях предотвращения утечек памяти с возможным отказом в обслуживании рекомендуем заблокировать автозагрузку следующих модулей ядра:

libertas_cs.ko
kalmia.ko
smsc75xx.ko
fan.ko
fotg210-udc.ko
udc-xilinx.ko
libertas_tf_usb.ko
usb8xxx.ko
avma1_cs.ko
ir-lirc-codec.ko
radio-maxiradio.ko
i5100_edac.ko
snd-cs5535audio.ko
snd-seq-dummy.ko
ems_pcmcia.ko
snd-korg1212.ko
snd-cs46xx.ko
snd-lola.ko
sis5595.ko
megaraid_mm.ko
lmc.ko
jsm.ko
ips.ko
amd5536udc.ko
hfcsusb.ko
hfc_usb.ko
virtio_pci.ko
hwa-rc.ko
ems_usb.ko
ddbridge.ko
dc395x.ko

Для этого в каталоге */lib/modprobe.d* в файлы

- ***/lib/modprobe.d/blacklist_linux_4.2.0-23-generic.conf***
- ***/lib/modprobe.d/ blacklist_linux_4.2.0-23-pax.conf***

внести строки, содержашие ключевое слово blacklist и название блокируемого модуля:

blacklist_linux_4.2.0-23-*.conf

```
blacklist libertas_cs.ko
blacklist kalmia.ko
blacklist smsc75xx.ko
blacklist fan.ko
blacklist fotg210-udc.ko
blacklist udc-xilinx.ko
blacklist libertas_tf_usb.
ko
blacklist usb8xxx.ko
blacklist avma1_cs.ko
blacklist ir-lirc-codec.ko
blacklist radio-maxiradio.
ko
blacklist i5100_edac.ko
```

```
blacklist snd-cs5535audio.
ko
blacklist snd-seq-dummy.ko
blacklist ems_pcmcia.ko
blacklist snd-korg1212.ko
blacklist snd-cs46xx.ko
blacklist snd-lola.ko
blacklist sis5595.ko
blacklist megaraid_mm.ko
blacklist lmc.ko
blacklist jsm.ko
blacklist ips.ko
blacklist amd5536udc.ko
blacklist hfcsusb.ko
blacklist hfc_usb.ko
blacklist virtio_pci.ko
blacklist hwa-rc.ko
blacklist ems_usb.ko
blacklist ddbridge.ko
blacklist dc395x.ko
```

После внесения и сохраения изменений:

1. Обновить ramfs командой

```
sudo update-initramfs -uk all
```

2. Перезагрузить систему.

БЮЛЛЕТЕНЬ № 20190529SE15MD

Методические указания не являются кумулятивным обновлением безопасности. При выполнении методических указаний автоматическая установка обновлений безопасности не осуществляется, и обновления безопасности должны быть установлены отдельно.

Методические указания по нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" (версия 1.5) в информационных системах.

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета **busybox**.
Для предотвращения эксплуатации указанной уязвимости необходимо ограничить доступ к утилите busybox всем, кроме пользователей, входящих в группу astra-admin,
для чего нужно выполнить от имени учетной записи администратора ОС СН с высоким уровнем целостности следующие команды:

```
chown root:astra-admin /bin/busybox
chmod g+rx /bin/busybox
chmod o-rx /bin/busybox
```

БЮЛЛЕТЕНЬ № 20190329SE15

Кумулятивное обновление (содержит в себе обновления `31082018SE15, 29032017SE15,16092016SE15,27102017SE15,02032018SE15 27082018SE15`) для нейтрализации угроз эксплуатации и уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5). Необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.

Обновление диска со средствами разработки

Соответствующее бюллетеню № 20190329SE15 обновление диска со средствами разработки доступно по ссылке

1. Загрузить образ диска с обновлениями по ссылке

Скачать

2. Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/20190329SE15.iso
```

Контрольная сумма:

f0a193280a5314bab8243d13463fed4ffd40f7981f5b86c1ca34a9e05354c57f -

Обновление безопасности подписано усиленной квалифицированной электронной подписью АО "НПО РусБИТех", выданной удостоверяющим центром Министерства Обороны Российской Федерации (Скачать). Для проверки подписи необходимо добавить в локальное хранилище сертификаты головного удостоверяющего центра и списки отозванных сертификатов, размещенные на сайте: https://structure.mil.ru/structure/UC/certificate.htm

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск

операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)

3. выполнить команды:

```
sudo mount /mnt/20190329SE15.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "20190329SE15"

Внимание

На время установки обновления необходимо снять запрет на установку бита исполнения в политиках безопасности.

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-int-check необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

```
apt
CVE-2019-3462

bind9
CVE-2018-5740, CVE-2018-5745, CVE-2019-6465

busybox
CVE-2011-5325, CVE-2013-1813, CVE-2014-4607,CVE-2014-9645,
CVE-2015-9261, CVE-2016-2147, CVE-2016-2148, CVE-2017-15873,
CVE-2017-16544, CVE-2018-1000517, CVE-2011-5325, CVE-2015-9261

cups
CVE-2018-4180, CVE-2018-4181

curl
CVE-2018-14618, CVE-2018-16842

elfutils
CVE-2017-7608, CVE-2017-7610, CVE-2017-7611,CVE-2017-7612,
CVE-2017-7613, CVE-2018-16062, CVE-2018-18310, CVE-2018-18520,
CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7665

exiv2
CVE-2018-10958, CVE-2018-10998, CVE-2018-10999,CVE-2018-11531,
CVE-2018-12264, CVE-2018-12265
```

```
fuse
CVE-2018-10906

ghostscript
CVE-2018-11645

gnupg
CVE-2016-6313, CVE-2017-7526, CVE-2018-12020

gnutls26
CVE-2017-7869, CVE-2017-5335, CVE-2017-5336,CVE-2017-5337

krb5
CVE-2015-2694, CVE-2016-3119, CVE-2016-3120,CVE-2017-11368,
CVE-2018-5729, CVE-2018-5730, CVE-2018-20217

lame
CVE-2017-9870, CVE-2017-9871, CVE-2017-9872,CVE-2017-15018,
CVE-2017-15045, CVE-2017-15046

lcms
CVE-2018-16435

lcms2
CVE-2018-16435

libapache2-mod-perl2
CVE-2011-2767

libarchive
CVE-2017-14501, CVE-2017-14502, CVE-2017-14503,
CVE-2019-1000019, CVE-2019-1000020

libcaca
CVE-2018-20544, CVE-2018-20546, CVE-2018-20547,
CVE-2018-20549

libsdl1.2
CVE-2019-7572, CVE-2019-7573, CVE-2019-7574,CVE-2019-7575,
CVE-2019-7576, CVE-2019-7577, CVE-2019-7578, CVE-2019-7635,
CVE-2019-7636, CVE-2019-7637, CVE-2019-7638

libsndfile
CVE-2017-14245, CVE-2017-14246, CVE-2017-14634,
CVE-2017-17456, CVE-2017-17457, CVE-2018-13139,
CVE-2018-19661, CVE-2018-19662, CVE-2018-19758

libtirpc
CVE-2018-14622

libxcursor
CVE-2015-9262

libxml2
CVE-2018-14404, CVE-2018-14567, CVE-2018-9251,CVE-2017-18258

linux
CVE-2018-5391, CVE-2018-1000026, CVE-2019-7221,
CVE-2019-7222,CVE-2019-6974, CVE-2018-20784

ming
CVE-2018-11226, CVE-2018-11225, CVE-2018-11100, CVE-2018-11095

mutt
CVE-2018-14349, CVE-2018-14350, CVE-2018-14351, CVE-2018-14352,
CVE-2018-14353, CVE-2018-14354, CVE-2018-14355,CVE-2018-14356,
CVE-2018-14357, CVE-2018-14358, CVE-2018-14359, CVE-2018-14362

mysql
CVE-2018-2767, CVE-2018-3058, CVE-2018-3063,CVE-2018-3066,
CVE-2018-3070, CVE-2018-3081, CVE-2018-3133, CVE-2018-3174,
CVE-2018-3282

net-snmp
CVE-2018-18065

nss
CVE-2018-12404, CVE-2018-18508

openssh
CVE-2018-15473

openssl
CVE-2018-0732, CVE-2018-0737, CVE-2018-0735, CVE-2018-5407,
```

```
CVE-2019-1559

perl
CVE-2018-12015, CVE-2018-18311

php5
CVE-2018-14851, CVE-2018-14883, CVE-2018-17082,
CVE-2018-19518, CVE-2018-19935,CVE-2018-20783, CVE-2018-1000888,
CVE-2019-9022,CVE-2019-9637, CVE-2019-9638, CVE-2019-9639,
CVE-2019-9640, CVE-2019-9641

pixman
CVE-2018-5297

python2.7
CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647

ruby-passenger
CVE-2018-12029

samba
CVE-2016-2125, CVE-2017-2619, CVE-2017-7494, CVE-2018-10858,
CVE-2018-16851

spice
CVE-2018-10873, CVE-2019-3813

sqlite3
CVE-2017-2518, CVE-2018-8740, CVE-2018-20346

systemd
CVE-2018-1049, CVE-2018-15686

tar
CVE-2018-20482

tiff3
CVE-2017-11613, CVE-2018-5784, CVE-2018-18557

tiff
CVE-2018-10963, CVE-2018-1710x, CVE-2018-18557, CVE-2018-18661,
CVE-2018-10779, CVE-2018-12900, CVE-2018-17000,
CVE-2018-19210, CVE-2019-6128
```

БЮЛЛЕТЕНЬ № 31082018SE15

Кумулятивное обновление (содержит в себе обновление `29032017SE15,16092016SE15,27102017SE15,02032018SE15 27082018SE15`) для нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5). Необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.

Обновление диска со средствами разработки

Соответствующее бюллетеню № 31082018SE15 обновление диска со средствами разработки доступно по ссылке

1. Загрузить образ диска с обновлениями по ссылке

Скачать

2. Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/31082018se15.iso
```

Контрольная сумма:

```
c46e22dd4ec1ff0254d3ca9d258fce6c0cbbfc771e623e7dc1260f0c2ef56185 -
```

Обновление безопасности подписано усиленной квалифицированной электронной подписью АО "НПО РусБИТех", выданной удостоверяющим центром Министерства Обороны Российской Федерации (Скачать). Для проверки подписи необходимо добавить в локальное хранилище сертификаты головного удостоверяющего центра и списки отозванных сертификатов, размещенные на сайте: https://structure.mil.ru/structure/UC/certificate.htm

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск

операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)

3. выполнить команды:

```
sudo mount /mnt/31082018se15.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "31082018se15"

Внимание

На время установки обновления необходимо снять запрет на установку бита исполнения в политиках безопасности.

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание!

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-int-check необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

1. **Aldd, ald-parsec**

   Astra-ald-2018-01

2. **Apache2**

   CVE-2018-1312

3. **Beep**

   CVE-2018-0492

4. **Bind9**

   CVE-2017-3145

5. **Cups**

   CVE-2017-18190

6. **Curl**

   CVE-2018-1000301

7. **Dovecot**

   CVE-2017-14461

8. **Eglibc**

   CVE-2018-1000001

9. **File**

   CVE-2018-10360

10. **Firefox-esr**

    CVE-2018-5183

11. Fly-dm

Astra-fly-2018-02

12. Fly-wm

Astra-fly-2018-03

13. Freerdp

CVE-2017-2839

14. Ghostscript

CVE-2018-10194

15. Gimp

CVE-2017-17784, CVE-2017-17785, CVE-2017-17786, CVE-2017-17787, CVE-2017-17788, CVE-2017-17789

16. Git

CVE-2018-11235

17. Graphicsmagick

CVE-2018-9018

18. Icu

CVE-2017-15422

19. Imagemagick

CVE-2018-11251

20. Isc-dhcp

CVE-2018-5732

21. Libgd2

CVE-2018-5711

22. Libmad

CVE-2017-8374

23. Libparsec-common-qt5

Astra-prsc-2018-04

24. Librsvg

CVE-2018-1000041

25. Libvirt

CVE-2018-5748

26. Libvncserver

CVE-2018-7225

27. Libvorbis

CVE-2018-5146

28. Libvpx

CVE-2017-13194

29. Memcached

CVE-2018-1000127

30. Mercurial

CVE-2018-1000132

31. Net-snmp

CVE-2018-1000116

32. Openslp-dfsg

CVE-2017-17833

33. Openssh

CVE-2016-10708

34. Openssl

CVE-2018-0739

35. Patch

CVE-2018-1000156

36. Perl

CVE-2018-6913

37. Php5

CVE-2018-10548

38. Postgresql

Astra-psql-2018-05

39. Postgresql-common

Astra-psql-2018-06

40. Procps

CVE-2018-1125

41. Python-crypto

CVE-2018-6594

42. Python-django

CVE-2018-7537

43. Qemu

CVE-2018-7550

44. Rsync

CVE-2018-5764

45. Ruby1.9.1

CVE-2018-1000075, CVE-2018-1000076, CVE-2018-1000077, CVE-2018-1000078

46. Sdl-image1.2

CVE-2017-14450

47. Squid

CVE-2018-1000027

48. Wget

CVE-2018-0494

49. Xorg-server

Astra-Xorg-2018-07

БЮЛЛЕТЕНЬ № 27082018SE15

Для предотвращения возможности подключения отчуждаемых носителей в нарушение установленных политик безопасности дискреционного разграничения доступа необходимо в папку */etc/polkit-1/localauthority/10-vendor.d/* поместить файл *ru.rusbitech.noudisksmount.pkla* со следующим содержимым:

/etc/polkit-1/localauthority/10-vendor.d/ru.rusbitech.noudisksmount.pkla

```
[Disable mount for limited users]
 Identity=unix-user:*
 Action=org.freedesktop.udisks.filesystem-mount
 ResultActive=auth_admin
```

БЮЛЛЕТЕНЬ № 02032018SE15

Кумулятивное обновление (содержит в себе обновления №27102017SE15,№29032017SE15, №16092016SE15) для нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5). Для минимизации рисков эксплуатации уязвимостей микропроцессоров Meltdown (CVE-2017-5754) и Spectre v2 (CVE-2017-5715) в состав данного обновления включено ядро linux 4.2.0-24.

Обновление диска со средствами разработки

Соответствующее бюллетеню № 02032018SE15 обновление диска со средствами разработки доступно по ссылке

В связи с серьезными изменениями в части своего интерфейса это ядро устанавливается дополнительно к linux 4.2.0-23 и не загружается по умолчанию. Стороннее программное обеспечение, содержащее в своем составе модули ядра, скомпилированные для ядра 4.2.0-23, может работать некорректно и потребовать перекомпиляции.

1. В файле /etc/default/grub заменить строку

```
#GRUB_DEFAULT=0
```

строкой

```
GRUB_DEFAULT=0
```

и заменить строку

```
GRUB_DEFAULT=version
```

строкой

```
#GRUB_DEFAULT=version
```

2. Выполнить команду:

```
update-grub
```

Также для повышения безопасности при эксплуатации операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01, рекомендуется выполнить дополнительные настройки, размещенные в разделе Astra Linux SE (ОС СН) Смоленск 1.5 Red-Book.

Необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.

1. Загрузить образ диска с обновлениями по ссылке

Скачать

2. Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/02032018se15.iso
```

Контрольная сумма:

```
3f05fae712288a5d65d16b141a95a16726031fa76409a7910847a389f8226627
```

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск
операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)

3. выполнить команды:

```
sudo mount /mnt/02032018se15.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "02032018SE15"

Внимание

На время установки обновления необходимо снять запрет на установку SUID бита в политиках безопасности.

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание!

В случае, если на компьютере установлена СУБД PostgreSQL из состава операционной системы, после обновления необходимо выполнить:

```
sudo chmod +x /usr/share/postgresql-common/pg_ctlcluster
sudo apt-get -f install
```

Внимание!

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-int-check необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

1. Apr

CVE-2017-12613, CVE-2017-12618

2. Db

CVE-2017-10140

3. Curl

CVE-2017-8817, CVE-2017-1000257

4. Eglibc

CVE-2016-3706, CVE-2018-1000001

5. Erlang

CVE-2017-1000385

6. Evince

CVE-2017-1000159

7. Exiv2

CVE-2017-11591, CVE-2017-11683, CVE-2017-14859

8. Firefox

CVE-2017-7828, CVE-2017-7826, CVE-2017-7830, CVE-2017-7843

9. Gdk-pixbuf

CVE-2017-1000422

10. GraphicsMagick

CVE-2017-17498, CVE-2017-17500, CVE-2017-17501, CVE-2017-17502, CVE-2017-17503, CVE-2017-17782, CVE-2017-17912, CVE-2017-17915

CVE-2017-13134, CVE-2017-16547, CVE-2017-16669, CVE-2017-16352, CVE-2017-16353, CVE-2017-15930, CVE-2017-13737, CVE-2017-15277

CVE-2017-14103, CVE-2017-14314, CVE-2017-14504, CVE-2017-14733, CVE-2017-14994, CVE-2017-14997

11. Icu

CVE-2017-14952

12. Imagemagick

CVE-2017-1000445, CVE-2017-1000476

CVE-2017-17914, CVE-2017-17879, CVE-2017-17682, CVE-2017-17504, CVE-2017-13768, CVE-2017-13769, CVE-2017-14060, CVE-2017-14172

CVE-2017-14173, CVE-2017-14174, CVE-2017-14175, CVE-2017-14224, CVE-2017-14249, CVE-2017-14341, CVE-2017-14400, CVE-2017-14505

CVE-2017-14607, CVE-2017-14682, CVE-2017-14739, CVE-2017-14741, CVE-2017-14989, CVE-2017-15016, CVE-2017-15017, CVE-2017-15277

CVE-2017-15281, CVE-2017-12691, CVE-2017-12692, CVE-2017-12693, CVE-2017-12875, CVE-2017-13758

13. Libwpd

CVE-2017-14226

14. Libxcursor

CVE-2017-16612

15. Libxfont

CVE-2017-13720, CVE-2017-13722

16. Libxi

CVE-2016-7945, CVE-2016-7946

17. Libxml2

CVE-2017-5130, CVE-2017-15412, CVE-2017-16931, CVE-2017-16932

18. Linux

CVE-2017-5715, CVE-2017-5754, CVE-2018-1000026

19. Linux-astra-modules

ASTRA-LAM-2017-01, ASTRA-LAM-2017-02, ASTRA-LAM-2017-03

20. Linux-firmware

CVE-2017-13081

21. Linx-cur

CVE-2017-1000211

22. mercurial

CVE-2017-17458

23. NSS

CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-7805

24. Openssl

CVE-2017-3735

25. Parsec

ASTRA-PRSC-2017-04, ASTRA-PRSC-2017-05, ASTRA-PRSC-2017-06

26. PostgreSQL

CVE-2017-12172, CVE-2017-15098, CVE-2017-7484, CVE-2017-7485, CVE-2017-7486, CVE-2017-7547, CVE-2017-7546, CVE-2017-7548

27. Procmail

CVE-2017-16844

28. Python

CVE-2017-1000158

29. Rsync

CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

30. Ruby

CVE-2017-17405, CVE-2017-17790

31. Sdl-image

CVE-2017-2887

32. Sensible-utils

CVE-2017-17512

33. Thunderbird

CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

CVE-2017-7793, CVE-2017-7805, CVE-2017-7810, CVE-2017-7814, CVE-2017-7818, CVE-2017-7819, CVE-2017-7823, CVE-2017-7824

CVE-2017-7753, CVE-2017-7779, CVE-2017-7784, CVE-2017-7785, CVE-2017-7786, CVE-2017-7787, CVE-2017-7791, CVE-2017-7792, CVE-2017-7800, CVE-2017-7801, CVE-2017-7802, CVE-2017-7803, CVE-2017-7807, CVE-2017-7809

CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778

CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5437, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467 CVE-2017-5469

34. Wget

CVE-2017-13090, CVE-2017-13089

35. Xen

CVE-2017-17044, CVE-2017-17045, CVE-2017-17566, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-15589, CVE-2017-15595 , CVE-2017-15588

CVE-2017-15593 ,CVE-2017-15592 ,CVE-2017-10912 , CVE-2017-10913, CVE-2017-10914 ,CVE-2017-10915 ,CVE-2017-10918

CVE-2017-10920, CVE-2017-10921, CVE-2017-10922 , CVE-2017-12135 ,CVE-2017-12137 ,CVE-2017-12855, CVE-2017-14316

CVE-2017-14318 ,CVE-2017-14317 ,CVE-2017-14319 , CVE-2017-17565

36. Xrdp

CVE-2017-16927

37. C-ares

CVE-2017-1000381

БЮЛЛЕТЕНЬ № 27102017SE15

Кумулятивное обновление (содержит в себе обновление 29032017SE15 и 16092016SE15) для нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5). Необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.

1. Загрузить образ диска с обновлениями по ссылке

Скачать

2. Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/27102017se15.iso
```

Контрольная сумма:

```
c079dff8ed74e1dc0f2c91dd5ad73db4fee2c0af1b7a741f530a679e9e6b07d7
```

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск
операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)

3. выполнить команды:

```
sudo mount /mnt/27102017se15.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "27102017SE15"

Внимание

На время установки обновления необходимо снять запрет на установку SUID бита в политиках безопасности.

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание!

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-int-check необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

1. Apache

CVE-2017-3167

CVE-2017-3169

CVE-2017-7668

CVE-2017-7669

CVE-2017-9798

CVE-2017-9788

2. Augeas

CVE-2017-7555

3. Bind9

CVE-2017-3143

4. Bluez

CVE-2017-1000250

5. c-ares

CVE-2016-0729

6. Curl

CVE-2017-1000254

CVE-2017-1000100

7. Cvs

CVE-2017-12836

8. Dnsmasq

CVE-2017-14494

9. expat

CVE-2017-9233

10. Evince

CVE-2017-1000083

11. Faad2

CVE-2017-9257

12. Firefox

CVE-2017-7793, ...

13. Fontforge

CVE-2017-11568, ...

14. Freexl

CVE-2017-2924, CVE-2017-2923

15. fly-wm

Уязвимость fly-wm, приводящая к аварийному завершению приложения.

16. Gdk-pixbuf

CVE-2017-2862

17. Ghostscript

CVE-2017-11714

18. git

CVE-2017-8386

CVE-2017-1000117

19. gtk

CVE-2013-7447

20. GraphicsMagick

CVE-2017-13777

21. Graphlite2

CVE-2017-13777

22. Heimdal

CVE-2017-11103

23. imagemagick

CVE-2017-9261

CVE-2017-9262

CVE-2017-9405

CVE-2017-9407

CVE-2017-9409

CVE-2017-9439, CVE-2017-9500, CVE-2017-9501

CVE-2017-13658

24. imlib2

CVE-2011-5326

CVE-2016-3993

CVE-2016-3994

CVE-2016-4024

25. libarchive

CVE-2016-7166

26. libffi

CVE-2017-1000376

27. Libflycore

Уязвимость в libflycore до версии 2.2.14, позволяющая злоумышленнику вызвать отказ в обслуживании.

28. libgcrypt11

CVE-2017-7526

29. libgd2

CVE-2017-7890

30. libgxps

CVE-2017-11590

31. Libidn

CVE-2017-14062

32. Libmtp

CVE-2017-9832

33. libmwaw

CVE-2017-9433

34. libsndfile

CVE-2017-6892

CVE-2017-12562

35. libtasn1

CVE-2017-10790

36. Libxml2

CVE-2017-7376

CVE-2017-9049, CVE-2017-9050

37. Linux

CVE-2017-7533

CVE-2017-1000380

38. linux-astra-modules

Уязвимость в linux-astra-modules, позволяющая локальному пользователю нарушить целостность данных.

39. memcached

CVE-2017-9951

40. mercurial

CVE-2017-9462

CVE-2017-1000116

41. openexr

CVE-2017-9116

42. openvpn

CVE-2017-7520

43. p7zip

CVE-2016-2335

44. parsec

Уязвимость модуля безопасности parsec, позволяющая вызвать отказ в обслуживании.

45. Perl

CVE-2017-6512

46. PHP

CVE-2017-11147

47. Qemu

CVE-2017-15038

48. rubygems

CVE-2017-0901

49. sane-backends

CVE-2017-6318

50. spice

CVE-2017-7506

51. sqlite3

CVE-2017-10989

52. Subversion

CVE-2017-9800

53. thunderbird

CVE-2016-1935

54. tiff

CVE-2017-10688

55. unzip

cve-2014-9913, cve-2016-9844

56. vim

CVE-2017-11109

57. vorbis

CVE-2015-6749

58. wpa

CVE-2017-13077,

Множественные уязвимости в wpa, позволяющие удаленному нарушителю получить доступ к зашифрованной конфиденциальной информации.

59. yodl

CVE-2016-10375

БЮЛЛЕТЕНЬ № 01062017SE15

Методические указания по нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" (версия 1.5) в информационных системах.

Методика безопасности, нейтрализующая уязвимость CVE-2017-7494

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета **samba**. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН добавить строку:

/etc/samba/smb.conf

```
nt pipe support = no
```

в секцию **[global]** конфигурационного файла */etc/samba/smb.conf*

БЮЛЛЕТЕНЬ № 29032017SE15

Кумулятивное обновление (содержит в себе обновление № 16092016SE15) для нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5). Необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.
1. Загрузить образ диска с обновлениями по ссылке
Скачать
2. Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/29032017se15.iso
```

Контрольная сумма:

```
093cd34500d1070cd9ef6d9367e230d45b82d890e89237aeaa8fcc1d1acd395c
```

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск
операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)

Контрольная сумма iso-образа обновления безопасности № 29032017se15, рассчитанная с использованием Программы фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0» 643.53132931.501492-01 (далее по тексту — программа «ФИКС-UNIX 1.0») по алгоритму «Уровень-3», должна соответствовать значению:

C74BE35C

Подсчет контрольной суммы iso-образа обновления безопасности № 29032017se15 с использованием программы «ФИКС-UNIX 1.0» по алгоритму «Уровень-3» должен осуществляться пользователем с правами администратора на рабочей станции, под управлением ОС СН «Astra Linux Special Edition» РУСБ.10015-01, в следующей

последовательности:

Поместить загруженный iso-образ в каталог */mnt* на обновляемой системе;

Выполнить в командной строке:

```
sudo mount /mnt/29032017se15.iso /media/cdrom
```

Перейти в директорию, содержащую исполняемый модуль программы «ФИКС-UNIX 1.0» (ufix), и выполнить следующие команды:

```
./ufix -jR /media/cdrom > /tmp/29032017se15.txt

./ufix -e /tmp/29032017se15.txt /tmp/29032017se15.prj

./ufix -h /tmp/29032017se15.prj /tmp/29032017se15_Report.html
```

Выполнить в командной строке:

```
firefox /tmp/29032017se15_Report.html
```

Сравнить значение контрольной суммы в строке «ВСЕГО», выданное на экран, со значением, указанным выше

---

3. выполнить команды:

```
sudo mount /mnt/29032017se15.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "29032017se15"

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание!

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-int-check необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

Примечание

После установки обновления, если запущен контроллер домена, необходимо выполнить команду:
`ald-init restart`
для контроллера домена, и:
`ald-client restart`
для клиента домена.

1. Kernel
CVE-2017-2636, CVE-2017-7184, CVE-2016-10229
2. Apache
CVE-2016-5387
3. Bash
CVE-2016-7543
4. Bind9
CVE-2016-1285
CVE-2016-1286
CVE-2016-2775
CVE-2016-2776
CVE-2016-2848
CVE-2016-8864
CVE-2016-9131, CVE-2016-9147, CVE-2016-9444
5. Binutils
CVE-2016-2226
6. Firebird2.5
Ошибка из-за отсутствия проверки длинны имени файла
7. Firefox
CVE-2016-9080, CVE-2016-9893, CVE-2016-9894, CVE-2016-9895, CVE-2016-9896, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9901, CVE-2016-9902, CVE-2016-9903, CVE-2016-9904
8. Ghostscript
CVE-2016-8602
CVE-2013-5653
CVE-2016-7976
CVE-2016-7977
CVE-2016-7978
CVE-2016-7979
9. GraphicsMagick
CVE-2016-7448
CVE-2016-7996
CVE-2016-7997
CVE-2016-8682
CVE-2016-8683
CVE-2016-8684
CVE-2016-7446
CVE-2016-7447
CVE-2016-7449
CVE-2016-7800
CVE-2016-5240
CVE-2016-5241
CVE-2016-5118
10. Gstreamer
10.1.CVE-2016-9634, CVE-2016-9635
10.2.CVE-2016-9811
11. Iproute
Аварийное завершение утилиты из-за некорректной обработки входных параметров
12. Krb5
Ошибка передачи контекста безопасности
13. Librsvg
CVE-2015-7558, CVE-2016-4347, CVE-2016-4348
CVE-2015-7557
14. Libxml2
CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4449, CVE-2016-4483, CVE-2015-8806
CVE-2016-4658
CVE-2016-5131
15. Ntfs-3g
CVE-2017-0358
CVE-2015-3202
16. Ntp
CVE-2015-7974

CVE-2015-7977, CVE-2015-7978
CVE-2015-7979
CVE-2015-8138
CVE-2015-8158
CVE-2016-1548
CVE-2016-1550
CVE-2016-2516
CVE-2016-2518

17. Openssh

CVE-2016-6515
CVE-2015-8325

18. Openssl

CVE-2016-2177
CVE-2016-2178
CVE-2016-2179
CVE-2016-2180
CVE-2016-2181
CVE-2016-2183
CVE-2016-6302
CVE-2016-6303
CVE-2016-6304
CVE-2016-6306

19. Perl

CVE-2016-1238

20. PHP

CVE-2016-2554
CVE-2016-4473, CVE-2016-4538, CVE-2016-5114, CVE-2016-5399, CVE-2016-5768, CVE-2016-5769, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297
CVE-2016-7411
CVE-2015-8865, CVE-2015-8866, CVE-2015-8878, CVE-2015-8879, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4343, CVE-2016-4537, CVE-2016-4539, CVE-2016-4540, CVE-2016-4541, CVE-2016-4542, CVE-2016-4543, CVE-2016-4544
CVE-2016-9934
CVE-2016-9935
CVE-2016-10158
CVE-2016-10159
CVE-2016-10160
CVE-2016-10161

21. Postgresql

Ошибка обработки входных данных, позволяющая вызвать аварийное завершение утилиты или получить доступ к конфиденциальной информации

22. Postgresql-common

Ошибка, позволяющая вызвать аварийное завершение утилиты из-за некорректной обработки входных параметров

23. Speech-tools

Ошибка, связанная с отсутствием проверки имени файла, указанного в качестве параметра, и его длинны

24. Squid

CVE-2016-4554

25. Subversion

CVE-2016-2167
CVE-2016-2168

26. Sudo

CVE-2016-7032, CVE-2016-7076

27. Textlive-bin

Ошибка, связанная с отсутствием проверки имени и файла, указанного в качестве параметра

28. Boost1.49

CVE-2012-2677

29. C-ares

CVE-2016-5180

30. Cracklib2

CVE-2016-6318

31. Curl

CVE-2016-9586

CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619,
CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624
CVE-2016-7167
CVE-2016-7141
CVE-2016-5419
CVE-2016-5420

32. Dpkg

CVE-2015-0860

33. Expat

CVE-2012-6702, CVE-2016-5300
CVE-2015-1283
CVE-2016-0719

34. File

CVE-2015-8865

35. Fly-wm

Аварийное завершение сессии пользователя из-за некорректной обработки закрытия иерархии окон типа: главное окно, транзиентное окно, транзиентное окно

36. Gdk-pixbuf

CVE-2015-7552
CVE-2015-7674

37. Giflib

CVE-2015-7555

38. Gimp

CVE-2016-4994

39. Git

CVE-2016-2324, CVE-2016-2315

40. GTK+3.0

CVE-2013-7447

41. Hdf5

CVE-2016-4330, CVE-2016-4331, CVE-2016-4332, CVE-2016-4333

42. Hesiod

CVE-2016-10151
CVE-2016-10152

43. Icu

CVE-2014-9911
CVE-2016-6293
CVE-2016-7415

44. Jansson

CVE-2016-6293

45. Jasper

CVE-2016-8654, CVE-2016-8691, CVE-2016-8692, CVE-2016-8693, CVE-2016-8882,
CVE-2016-8883, CVE-2016-8887, CVE-2016-9560
CVE-2016-1577
CVE-2016-2089
CVE-2016-2116
CVE-2016-1577

46. Kcoreaddons

CVE-2016-7966

47. Lcms2

CVE-2016-10165

48. Libass

CVE-2016-7972
CVE-2016-7969

49. Libcrypto++

CVE-2016-9939
CVE-2016-3995

50. Libebml

CVE-2015-8789
CVE-2015-8790, CVE-2015-8791

51. Libevent

CVE-2016-10197
CVE-2016-10195

52. Libflycore

Аварийное завершение программы из-за возможного переполнения буфера

53. Libgc

CVE-2016-9427
54. Libgcrypt
CVE-2016-6313
CVE-2015-7511
55. Libgd2
CVE-2016-6906, CVE-2016-6912, CVE-2016-9317, CVE-2016-10166, CVE-2016-10167, CVE-2016-10168
56. Libgsf
CVE-2016-9888
57. Libidn
CVE-2016-6263
CVE-2016-6261
CVE-2016-8948
CVE-2015-2059
58. Libmatroska
CVE-2015-8792
59. Libotr
CVE-2016-2851
60. Libplist
CVE-2017-5209
CVE-2017-5545
61. Libtasn
CVE-2016-4008
62. Libupnp
CVE-2016-8863
CVE-2016-6255
63. Libvirt
CVE-2016-5008
64. Libvncserver
CVE-2016-9941, CVE-2016-9942
65. Libwmf
CVE-2016-9011
66. Libx11
CVE-2016-7942, CVE-2016-7943
67. Libxfixes
CVE-2016-7944
68. Libxpm
CVE-2016-4658
69. LibXrand
CVE-2016-7947
CVE-2016-7948
70. Libxrender
CVE-2016-7949, CVE-2016-7950
71. Libxslt
CVE-2016-4738
72. Libxtst
CVE-2016-7951
CVE-2016-7952
73. Libxvl
CVE-2016-5407
74. Libxvmc
CVE-2016-7953
75. Memcached
CVE-2013-7291
76. Memcached
CVE-2016-8704, CVE-2016-8705, CVE-2016-8706
77. Mercurial
CVE-2016-3105
CVE-2016-3630, CVE-2016-3068, CVE-2016-3069
78. nettle
CVE-2016-6489
79. nspr
CVE-2016-1951
80. nss
CVE-2016-9074
81. Ocaml

CVE-2015-8869
82. pcsc-lite
CVE-2016-10109
83. pykerberos
CVE-2015-3206
84. python-cripto
CVE-2013-7459
85. python-django
CVE-2016-9014
CVE-2016-7401
CVE-2016-2512
CVE-2016-2513
86. python-imaging
CVE-2016-9189
CVE-2016-9190
CVE-2016-0775, CVE-2016-2533
87. python-tornado
CVE-2014-9720
88. Python2.7
CVE-2016-0772
CVE-2016-5636
CVE-2016-5699
89. Qemu
CVE-2016-9921, CVE-2016-9922
90. samba
CVE-2016-2111
91. spice
CVE-2016-0749
CVE-2016-2150
92. sqlite3
CVE-2016-6153
93. squid3
CVE-2016-10002
94. systemd
CVE-2016-7796
95. shadow
CVE-2017-2616
96. texlive
CVE-2016-10243
97. tre
CVE-2016-8859
98. vim
CVE-2016-1248
CVE-2017-5953
99. wget
CVE-2016-4971
CVE-2017-6508
100. wpa
CVE-2015-5315
101. xen
CVE-2016-10024
CVE-2016-10013
102. xerces-c
CVE-2016-2099
CVE-2016-0729

БЮЛЛЕТЕНЬ № 16092016SE15

Для нейтрализации угроз эксплуатации уязвимостей операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5) в информационных системах необходимо выполнить обновление операционной системы в соответствии с инструкцией, приведенной ниже.
1. Загрузить образ диска с обновлениями по ссылке
Скачать
2. Поместить загруженный iso-образ в каталог /mnt на обновляемой системе и проверить соответствие контрольной суммы, выполнив команду:

```
gostsum -d /mnt/essential_and_additional_bin.iso
```

Контрольная сумма:

0fd8405aad2a729f5daac2c980109cdad3f78a4365eb2876416e0af70663c3d7

Обновление операционной системы необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы. Также в процессе обновления может потребоваться установочный диск операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (версия 1.5)
3. выполнить команды:

```
sudo mount /mnt/essential_and_additional_bin.iso /media/cdrom
sudo apt-cdrom -m add
```

на вопрос об имени диска ввести "Astra Linux Security Updates"

```
sudo apt-get update
sudo apt-get dist-upgrade
```

после выполнения указанных команд будет выполнено обновление операционной системы.

Внимание!

После успешного обновления проверку целостности программных пакетов утилитой fly-admin-incheck необходимо проводить только с помощью файла gostsum.txt, расположенного в корневом каталоге диска с обновлениями.

В случае, если по каким-то причинам провести обновление программных пакетов указанным выше способом невозможно, выполните методические указания приведенные ниже:

Идентификаторы уязвимостей соответствуют указанным в банке данных угроз безопасности информации ФСТЭК России

1. Методика безопасности, нейтрализующая уязвимость BDU:2016-01146

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета imagemagick, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН в конфигурационный файл /etc/ImageMagick/policy.xml в раздел <policymap> добавить строки:

```
<policy domain="coder" rights="none" pattern="EPHEMERAL" />
<policy domain="coder" rights="none" pattern="URL" />
<policy domain="coder" rights="none" pattern="HTTPS" />
<policy domain="coder" rights="none" pattern="MVG" />
<policy domain="coder" rights="none" pattern="MSL" />
<policy domain="coder" rights="none" pattern="FTP" />
<policy domain="coder" rights="none" pattern="HTTP" />
```

2. Методика безопасности, нейтрализующая уязвимость BDU:2016-01573

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета libgraphicsmagick3, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН в конфигурационном файле /usr/lib/GraphicsMagick-1.3.16/config/delegates.mgk удалить строку:

```
<delegate decode="gplt" command='"echo" "set size 1.25,0.62; set terminal postscript portrait color solid;
set outp ut \"%o\"; load \"%i\"" > "%u"; "gnuplot" "%u"' />
```

3. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01583

Эксплуатация уязвимости возможна только при наличии в операционной системе разрешения у пользователей на запуск программы сбора сетевой статистики lnstat. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск данной программы, выполнив в терминале команду:

```
chmod 750 /usr/bin/lnstat
```

4. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01584

Эксплуатация уязвимости возможна только при наличии в операционной системе разрешения у пользователей на запуск программы сбора сетевой статистики lnstat. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск данной программы, выполнив в терминале команду:

```
chmod 750 /usr/bin/lnstat
```

5. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01585

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета gpsd-clients, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск программы gpxlogger, выполнив в терминале команду:

```
chmod 750 /usr/bin/gpxlogger
```

6. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01586

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета speech-tools, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск программы wfst_run, выполнив в терминале команду:

```
chmod 750 /usr/bin/wfst_run
```

7. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01587

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета texlive-binaries, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск программы mendex, выполнив в терминале команду:

```
chmod 750 /usr/bin/mendex
```

8. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01588

Эксплуатация уязвимости возможна только при наличии в операционной системе установленного пакета firebird2.5-classic-common, который не устанавливается по умолчанию. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН запретить пользователям запуск программы gdef, выполнив в терминале команду:

```
chmod 750 /usr/bin/gdef
```

9. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01589

Эксплуатация уязвимости возможна только при наличии в операционной системе разрешения на автоматическую загрузку модуля ядра drivers/net/wireless/libertas/libertas_cs.ko. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН в терминале выполнить команду:

```
echo blacklist libertas_cs > /etc/modprobe.d/blacklist_libertas_cs.conf

update-initramfs -u -k all
```

10. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01590

Эксплуатация уязвимости возможна только при наличии в операционной системе разрешения на автоматическую загрузку модуля ядра drivers/net/usb/kalmia.ko. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН в терминале выполнить команду:

```
echo blacklist kalmia > /etc/modprobe.d/blacklist_kalmia.conf

update-initramfs -u -k all
```

11. Методика безопасности, нейтрализующая уязвимость BDU:Z-2016-01591

Эксплуатация уязвимости возможна только при наличии в операционной системе разрешения на автоматическую загрузку модуля ядра drivers/net/usb/smsc75xx.ko. Для предотвращения эксплуатации указанной уязвимости необходимо от имени учетной записи администратора ОС СН в терминале выполнить команду:

```
echo blacklist smsc75xx > /etc/modprobe.d/blacklist_smsc75xx.conf

update-initramfs -u -k all
```

Информируем всех потребителей, что в командном интерпретаторе bash обнаружены уязвимости, с использованием которых потенциально возможно нарушение установленных правил разграничения доступа.