Обновления безопасности Astra Linux Special Edition 1.5

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.

Список уязвимостей, закрываемых обновлением № 27102017SE15

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.

<details>
<summary>Список уязвимостей, закрываемых обновлением № 29032017SE15</summary>

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
</details>

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:

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

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.