

2021-0915SE47MD

Astra Linux Special Edition .10152-02 (4.7) .

- ,
- , avahi
- , firefox
 - , CVE-2021-23958
 - , CVE-2021-23954 CVE-2021-23960
 - , CVE-2021-23994
 - , CVE-2021-23995
 - , CVE-2021-23997
 - , CVE-2021-29952
 - , CVE-2021-29970
 - , CVE-2021-30547
- , firefox thunderbird
- , glibc
- , imagemagick
- , iptables
- , linuxptp
- , ntp
- , php
- , python
- , rpm
- , rsyslog
- , sane-backends
- , screen
- , squid
- , tar
-



, , 4.7.2 4.7.1.



« »

,



apache2	CVE-2021-26691
binutils	CVE-2017-13716
binutils	CVE-2018-12699
binutils	CVE-2021-3487
chromium	CVE-2021-30547
firefox	CVE-2021-23956
firefox	CVE-2021-23962
firefox	CVE-2021-23965
firefox	CVE-2021-29947
firefox	CVE-2021-23964
firefox	CVE-2021-23998
firefox	CVE-2021-29976
firefox	CVE-2021-23958
firefox	CVE-2021-23997
firefox	CVE-2021-29952

firefox	CVE-2021-23954
firefox	CVE-2021-23960
firefox	CVE-2021-23961
firefox	CVE-2021-23994
firefox	CVE-2021-23995
firefox	CVE-2021-29970
firefox	CVE-2021-30547
imagemagick	CVE-2021-20244
imagemagick	CVE-2021-20245
imagemagick	CVE-2021-20246
imagemagick	CVE-2021-20309
imagemagick	CVE-2021-20311
imagemagick	CVE-2021-20312
libtasn1-6	CVE-2018-1000654
libx11	CVE-2006-4447
xdm	CVE-2006-4447
xorg-server	CVE-2006-4447
xterm	CVE-2006-4447
xtrans	CVE-2006-4447
libxml2	CVE-2021-3517
snmptt	CVE-2020-24361
squid	CVE-2021-28662
sysstat	CVE-2019-19725
thunderbird	CVE-2021-23964
thunderbird	CVE-2021-23998
thunderbird	CVE-2021-29976
thunderbird	CVE-2021-23954
thunderbird	CVE-2021-23960
thunderbird	CVE-2021-23961
thunderbird	CVE-2021-23994
thunderbird	CVE-2021-23995
thunderbird	CVE-2021-29970
thunderbird	CVE-2021-30547
glibc	CVE-2021-33574
glibc	CVE-2019-1010022
exim	CVE-2020-28009
exim	CVE-2020-28010
exim	CVE-2020-28011
exim	CVE-2020-28013
exim	CVE-2020-28017
exim	CVE-2020-28018

exim	CVE-2020-28021
exim	CVE-2020-28022
exim	CVE-2020-28024
exim	CVE-2020-28026

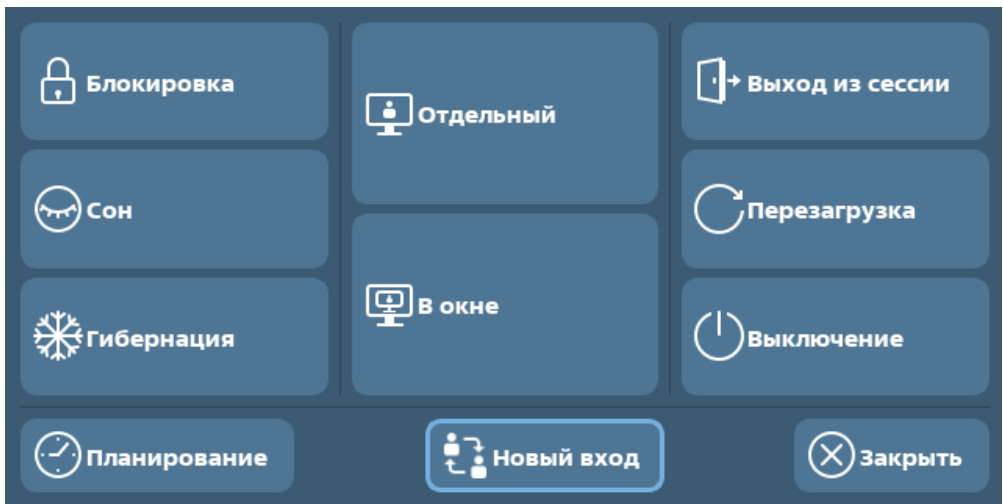
, , :

- () **Firejail**;



Firejail .10152-02 97 01-1 « «Astra Linux Special Edition». . 1».

- . — — . : (. .);



- , . -2, - . : [parsec-kiosk2](#) ();

- , , — bash;



bash , bash, .



bash bash .

« »

fly-admin-smc. :

- (): — — — ;
- — :
- Bash ;
- Bash ;
- — <Ctrl+S>.

(bash) :

sudo astra-interpreters-lock enable

, :

sudo astra-interpreters-lock status

, :

bash :

sudo astra-bash-lock enable

bash, :

sudo astra-bash-lock status

, :

- «» «» () :
 - 0;
 - 0;

« »

fly-admin-smc. :

- (): — — — ;
- ;
- ;
- — <Ctrl+S>.



.

:

`sudo astra-mic-control enable`



.

, :

`sudo astra-mic-control status`

, :

:

`sudo astra-digsig-control enable`



.

, :

`sudo astra-digsig-control status`

, :

- `<<>> <<>> — ( ) ( ) :`
`o , ;`
`o ;`

- `<<>> <<>> apache2 exim4 ( ). :`

```
sudo astra-ilev1-control enable
```

apache2 exim4, :

```
sudo astra-ilev1-control status
```

apache2 exim , :

, avahi



:

- CVE-2017-6519.

avahi (UDP 5353). :

iptables

, , :

```
sudo iptables -A INPUT -p udp --dport 5353 -j DROP
```



, . — . [iptables](#).

ufw

, :

```
sudo ufw deny 5353/udp
```

, firefox





:

- CVE-2021-23954;
- CVE-2021-23958;
- CVE-2021-23960;
- CVE-2021-23994;
- CVE-2021-23995;
- CVE-2021-23997;
- CVE-2021-29952;
- CVE-2021-29970;
- CVE-2021-30547.



firefox chromium.

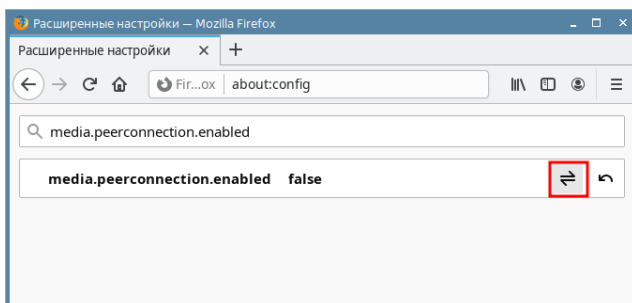
, (,).

, :

, CVE-2021-23958

WebRTC (), :

- , , : — — **Firefox**;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "media.peerconnection.enabled";
- false, [] ().



- - Firefox.

, CVE-2021-23954 CVE-2021-23960

JavaScript (), :

- , , : — — **Firefox**;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "javascript.enabled";
- false, [];
- - Firefox.

, CVE-2021-23994

WebGL (), :

- , , : — — **Firefox**;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "webgl.disabled";
- true, [];
- - Firefox.

, CVE-2021-23995

(), :

- , , : — — - Firefox;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "devtools.policy.disabled";
- true, [];
- - Firefox.

, CVE-2021-23997

, :

1. , , : — — - Firefox;
2. "about:config" <Enter>;
3. [Accept the Risk and Continue] ();
4. : "browser.cache.offline.enable";
5. false, [];
6. 4 5 :
 - browser.cache.disk.enable;
 - browser.cache.disk_cache_ssl;
 - browser.cache.memory.enable;
7. : "network.http.use-cache";
8. [+], false, [];
9. - Firefox.

, CVE-2021-29952

WebRender (), :

- , , : — — - Firefox;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "gfx.webrender.all";
- false, [];
- - Firefox.

, CVE-2021-29970

(Accessibility features), :

- , , : — — - Firefox;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "accessibility.force_disabled";
- "1";
- [];
- - Firefox.

, CVE-2021-30547

ANGLE (), :

- , , : — — - Firefox;
- "about:config" <Enter>;
- [Accept the Risk and Continue] ();
- : "webgl.disable-angle";
- true, [];
- - Firefox.

, firefox thunderbird



:

- CVE-2021-23961.



firefox chromium.

, (. ,).

TCP:-

- 6566 (SANE);
- 10080 (Amanda);
- 69 (TFTP);
- 161 (SNMP);
- 1719 (H323 (RAS));
- 137 (NetBIOS).

:

iptables

, , :

```
sudo iptables -A INPUT -p tcp --dport 6566 -j DROP
sudo iptables -A INPUT -p tcp --dport 10080 -j DROP
sudo iptables -A INPUT -p tcp --dport 69 -j DROP
sudo iptables -A INPUT -p tcp --dport 161 -j DROP
sudo iptables -A INPUT -p tcp --dport 1719 -j DROP
sudo iptables -A INPUT -p tcp --dport 137 -j DROP
```



, . —. [iptables](#).

ufw

, :

```
sudo ufw deny 6566/tcp
sudo ufw deny 10080/tcp
sudo ufw deny 69/tcp
sudo ufw deny 161/tcp
sudo ufw deny 1719/tcp
sudo ufw deny 137/tcp
```

, glibc



:

- CVE-2019-25013.

() EUC-KR.

, :

```
locale -a
```

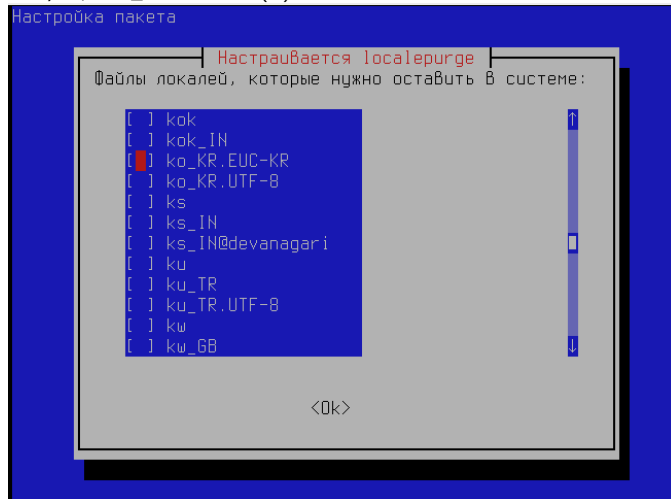
. EUC-KR, :

```
ko_KR.euckr
```

localepurge. :

```
sudo apt install localepurge
```

, , ko_KR.EUC-KR ().



, imagemagick



:

- CVE-2018-15607.

/etc/ImageMagick-6/policy.xml :

```
<policy domain="resource" name="width" value="10KP"/>
<policy domain="resource" name="height" value="10KP"/>
```

, iptables



:

- CVE-2012-2663.

iptables :

- «--syn» «--tcp-flags SYN,ACK,FIN SYN»;

- TCP-, SYN FIN;

```
sudo iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j REJECT
```



, . — . [iptables](#).

, linuxptp



:

- CVE-2021-3570.

:

- , (). ptp4l eno1:

```
sudo ptp4l -i eno1 -m -S
```

- — PTP, :

iptables

, , :

```
sudo iptables -A INPUT -p udp --dport 320 -j DROP
```



, . — . [iptables](#).

ufw

, :

```
sudo ufw deny 320/udp
```

- «» «» — () () :
○ , ;
○ .



linuxptp chronyd. : [chronyd](#).

, ntp



:

- CVE-2018-12327.

:

- IP- NTP-, :

```
sudo ntpdate -q < NTP->
```

NTP-, IP-.

, IP- NTP-, Whois-, web- <https://2ip.ru/whois/>.

IP- NTP- [ntp4.vniiftri.ru](https://2ip.ru/whois/) , :

- :

```
sudo ntpdate -q ntp4.vniiftri.ru
```

:

```
server 89.109.251.24, stratum 1, offset 1.294563, delay 0.03233
5 Aug 13:42:09 ntpdate[1640]: step time server 89.109.251.24 offset 1.294563 sec
```

- web- <https://2ip.ru/whois/> IP NTP- [].

, IP- (.).

IP	89.109.251.24
Хост:	ntp4.vniiftri.ru
Город:	Москва ⚠
Страна:	 Russian Federation
IP диапазон:	89.109.251.16 - 89.109.251.31
Название провайдера:	OJSC Rostelecom, Moscow region branch

- , NTP-.

 NTP- «», web- «» : <https://www.vniiftri.ru/catalog/services/sinkhronizatsiya-vremeni-cherez-ntp-servera/>.



ntp chronyd. : [chronyd](#).

, php



:

- CVE-2021-21702.

SOAP- PHP SOAP-. SOAP-, , , web- <https://www.virustotal.com/gui/home/url>.

, python



:

- CVE-2020-8492;
- CVE-2021-3177.

, (,).

, ctypes- PyCArg_repr , , sprintf, 256 . , , UTF-8, :

```
def utf8len (text):  
    return len(text.encode('utf-8'))
```

, rpm



:

- CVE-2010-2198;
- CVE-2010-2199;
- CVE-2017-7500.

rpm. **apt.** (DEB) **dpkg.**

RPM DEB **alien.** ():

```
sudo apt install alien
```

RPM DEB :

```
sudo alien < >.rpm
```

:

```
< >.deb generated
```

, rsyslog



:

- CVE-2019-17041;
- CVE-2019-17042.

() pmciscnames pmaixforwardedfrom. /etc/rsyslog.conf ("#") :

```
module(load="pmciscnames")
module(load="pmaixforwardedfrom")
```

, sane-backends



:

- CVE-2020-12861.

auto-discovery, /etc/sane.d/epsonds.conf ("#") :

```
net autodiscovery
```

, screen



:

- CVE-2021-26937.

screen , UTF-8. , KOI8-R (), :

- **screen**;
- **<Ctrl + A>**, " : ";
- **screen** :

```
defencoding KOI8-R
```

- **<Enter>**.

, squid



:

- BDU:2021-02727;
- CVE-2021-28652.

:

- HTTPS- ;

- , Cache Manager. /etc/squid/squid.conf , "allow", :

```
http_access deny manager
```

- Cache Manager, Cache Manager — , . — . - squid.

, tar



:

- CVE-2005-2541.

, (,).

, , , --no-same-permissions.

, , , :

- (sudo);
- , : --no-same-permissions

```
sudo tar zxvf file.tar.gz --no-same-permissions
```



, , .