

2022-0318E212MD

Astra Linux Common Edition 2.12, - Astra Linux, .

- , linux
 -
 -
 -
- - Firefox
 - Chromium
- , apache2
 - , lua_module , (multipart)
 - SSRF- (Server Side Request Forgery) mod_proxy
 - HTTP Request Smuggling
- liblog4j2-java
 -
 - JndiLookup

! , linux liblog4j2-java, , apache2.
, ca-certificates.deb Astra Linux .

! . .

! , , .

! Astra Linux 2.12.43

, linux

! . Astra Linux.

! ().

1. tar- WEB- : https://dl.astralinux.ru/astra/frozen/2.12_x86-64/2.12.43/iso/2022-0318CE212MD.tar.gz, :

```
wget https://dl.astralinux.ru/astra/frozen/2.12_x86-64/2.12.43/iso/2022-0318CE212MD.tar.gz
```

✓ "-":https://dl.astralinux.ru/astra/frozen/2.12_x86-64/2.12.43/iso/2022-0318CE212MD.tar.gz_2022-03-24_14-25-18.tsp.sig.

2. tar-;
3. , . :

```
gostsum 2022-0318CE212MD.tar.gz
```

:

```
b87de67a85bc7350e58801751aaa006eb0191caf824e0aa7c6d0225da3fa8679
```

4. , , /mnt/, :

```
sudo tar xzvf 2022-0318CE212MD.tar.gz -C /mnt/
```

5. tar- 2022-0318CE212MD (Astra Linux), , /mnt/2022-0318CE212MD/, :
 - /etc/apt/sources.list :

```
deb file:/mnt/2022-0318CE212MD/ ore1 main contrib non-free
```

- :

```
echo "deb file:/mnt/2022-0318CE212MD/ ore1 main contrib non-free"  
| sudo tee -a /etc/apt/sources.list
```

- :

```
sudo apt update
```

6. , :

```
sudo apt dist-upgrade
```



Firefox

1. , , : — — **Firefox**.
2. "about:preferences" <Enter>.
3. [].
4. [...].
5. /usr/share/ca-certificates/mozilla/rootca_MinDDC_rsa2022.crt [].
6. - [].
7. [].

, [] :

The Ministry of Digital Development and Communications
Russian Trusted Root CA

Chromium

1. , , : — — **Chromium**.
2. "chrome://settings/certificates" <Enter>.
3. [].
4. /usr/share/ca-certificates/mozilla/rootca_MinDDC_rsa2022.crt [].
5. [].

:

org-The Ministry of Digital Development and Communications
Russian Trusted Root CA

, **apache2**

, **lua_module** , (multipart)

LUA. , :

```
sudo apachectl -M
```

lua, :

```
sudo a2dismod lua
```

- Apache, :

```
sudo systemctl restart apache2
```

SSRF- (Server Side Request Forgery) mod_proxy

proxy (:/etc/apache2/sites-enabled/000-default.conf).

ProxyRequests "off". , , - .



, proxy, :

```
sudo a2dismod proxy
```

- Apache, :

```
sudo systemctl restart apache2
```

HTTP Request Smuggling

(:/etc/apache2/sites-enabled/000-default.conf) http2 — Protocols () "h2" (HTTP/2).

- Apache, :

```
sudo systemctl restart apache2
```

- Apache HTTPS.

liblog4j2-java



JndiLookup JAR /usr/share/java/log4j-core.jar, liblog4j2-java, JAR log4j-api JAR log4j-core, log4j 2.14.1 .

, liblog4j2-java :

```
apt policy liblog4j2-java
```

1. liblog4j2-java_2.7-2+deb9u1_all.deb WEB- ;
2. ;
3. :

```
sudo apt install ./liblog4j2-java_2.7-2+deb9u1_all.deb
```



"Download is performed unsandboxed"/" " , : "Download is performed unsandboxed"/" " apt

JndiLookup

, , /usr/share/java/log4j-core.jar, (JndiLookup) , :

1. zip, , :

```
sudo apt install zip
```

2. :

```
sudo zip -d /usr/share/java/log4j-core.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

:

```
deleting: org/apache/logging/log4j/core/lookup/JndiLookup.class
```