# RNS DATA AUTOMATION

## Apache Log4j Unsupported Version Detection

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-1 | During Vulnerability assessment and Penetration testing we observed that, According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Apache |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Upgrade to a version of Apache Log4j that is currently supported.  Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://www.nessus.org/u?59f655a2 |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Apache Log4j Unsupported Version Detection

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-2 | During Vulnerability assessment and Penetration testing we observed that, According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.175:0 10.101.101.176:0 | | Apache |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Upgrade to a version of Apache Log4j that is currently supported.  Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://www.nessus.org/u?59f655a2 |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Apache Log4j Unsupported Version Detection

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-3 | During Vulnerability assessment and Penetration testing we observed that, According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.175:0 10.101.101.176:0 10.101.101.174:0 | | Apache |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Upgrade to a version of Apache Log4j that is currently supported.  Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://www.nessus.org/u?59f655a2 |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : procps-ng (ELSA-2018-1700)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-4 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:1700 :  An update for procps-ng is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected procps-ng packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-May/007762.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libcdio (ELSA-2018-3246)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-5 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3246 :  An update for libcdio is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libcdio packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008208.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : perl (ELSA-2019-0109)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-6 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:0109 :  An update for perl is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected perl packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-January/008382.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : freerdp (ELSA-2019-0697)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-7 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:0697 :  An update for freerdp is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected freerdp packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-April/008620.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : wget (ELSA-2019-1228)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-8 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:1228 :  An update for wget is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected wget package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-May/008733.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : python (ELSA-2019-1587)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-9 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:1587 :  An update for python is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected python packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-June/008851.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : pango (ELSA-2019-2571)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-10 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:2571 :  An update for pango is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected pango packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-August/009087.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : ppp (ELSA-2020-0630)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-11 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:0630 :  An update for ppp is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected ppp packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-February/009666.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : curl (ELSA-2020-5562)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-12 | During Vulnerability assessment and Penetration testing we observed that, Description of changes:  [7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected curl packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-March/009685.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libpng (ELSA-2020-3901)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-13 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-3901 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libpng, libpng-devel and / or libpng-static packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3901.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libexif (ELSA-2020-5402)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-14 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-5402 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libexif, libexif-devel and / or libexif-doc packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-5402.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libX11 (ELSA-2021-3296)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-15 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-3296 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libX11, libX11-common and / or libX11-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-3296.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libxml2 (ELSA-2021-3810)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-16 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-3810 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-3810.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Apache Log4j 1.x Multiple Vulnerabilities

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-17 | During Vulnerability assessment and Penetration testing we observed that, According to its self-reported version number, the installation of Apache Log4j on the remote host is 1 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Apache |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Upgrade to a version of Apache Log4j that is currently supported.  Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://logging.apache.org/log4j/1.2/ |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : python (ELSA-2022-5235)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-18 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2022-5235 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-5235.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : systemd (ELSA-2022-6160)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-19 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-6160 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-6160.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : zlib (ELSA-2023-1095)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-20 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-1095 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1095.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libwebp (ELSA-2023-2077)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-21 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-2077 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-2077.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libssh2 (ELSA-2019-1884)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-22 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:1884 :  An update for libssh2 is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | SSH |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libssh2 packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-July/008928.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libexif (ELSA-2020-2549)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-23 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2549 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:2549 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libexif packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-June/010057.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libvorbis (ELSA-2018-1058)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-24 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:1058 :  An update for libvorbis is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libvorbis packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-April/007625.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : flatpak (ELSA-2018-2766)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-25 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:2766 :  An update for flatpak is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.6 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected flatpak packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-September/008050.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : samba (ELSA-2018-3056)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-26 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3056 :  An update for samba is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected samba packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008199.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libmspack (ELSA-2018-3327)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-27 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3327 :  An update for libmspack is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libmspack packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008205.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : NetworkManager (ELSA-2018-3665)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-28 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3665 :  An update for NetworkManager is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected networkmanager packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008287.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : ghostscript (ELSA-2019-3888)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-29 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:3888 :  An update for ghostscript is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected ghostscript packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-November/009343.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : nss / nss-softokn / nss-util (ELSA-2019-4190)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-30 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:4190 :  An update for nss, nss-softokn, and nss-util is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected nss, nss-softokn and / or nss-util packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-December/009446.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : sqlite (ELSA-2020-0227)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-31 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:0227 :  An update for sqlite is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected sqlite packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-January/009548.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : icu (ELSA-2020-0897)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-32 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:0897 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:0897 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected icu packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-March/009717.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : firefox (ELSA-2020-3253)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-33 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:3253 :  The remote Redhat Enterprise Linux 7 host has a package installed that is affected by multiple vulnerabilities as referenced in the RHSA-2020:3253 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9.3 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected firefox package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-July/010188.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : cups (ELSA-2020-3864)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-34 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2020-3864 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3864.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libtiff (ELSA-2020-3902)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-35 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2020-3902 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3902.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : gd (ELSA-2020-5443)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-36 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-5443 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected gd, gd-devel and / or gd-progs packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-5443.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libsndfile (ELSA-2021-3295)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-37 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-3295 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libsndfile, libsndfile-devel and / or libsndfile-utils packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-3295.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : webkitgtk4 (ELSA-2022-0059)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-38 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-0059 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-0059.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : cyrus-sasl (ELSA-2022-0666)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-39 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-0666 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-0666.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : gzip (ELSA-2022-2191)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-40 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by a vulnerability as referenced in the ELSA-2022-2191 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected gzip package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-2191.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : xz (ELSA-2022-5052)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-41 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-5052 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-5052.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : krb5 (ELSA-2022-8640)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-42 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-8640 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-8640.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : xorg-x11-server (ELSA-2023-0046)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-43 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2023-0046 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-0046.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libXpm (ELSA-2023-0377)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-44 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-0377 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libXpm and / or libXpm-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-0377.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : sssd (ELSA-2023-0403)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-45 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-0403 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-0403.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : nss (ELSA-2023-1332)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-46 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-1332 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1332.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : firefox (ELSA-2023-3137)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-47 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by multiple vulnerabilities as referenced in the ELSA-2023-3137 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected firefox package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-3137.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : firefox (ELSA-2023-3579)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-48 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by multiple vulnerabilities as referenced in the ELSA-2023-3579 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected firefox package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-3579.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 / 8 : vim (ELSA-2019-1619)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-49 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:1619 :  An update for vim is now available for Red Hat Enterprise Linux 7 and Red Hat Enterprise Linux 8 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9.3 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected vim packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-August/008984.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : icedtea-web (ELSA-2019-2003)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-50 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:2003 :  An update for icedtea-web is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected icedtea-web packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-July/008956.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : bind (ELSA-2020-2344)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-51 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2344 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:2344 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected bind packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-June/009985.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : perl (ELSA-2021-0343)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-52 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2021-0343 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-0343.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2020-2968)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-53 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2968 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:2968 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected java-1.8.0-openjdk packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-July/010137.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : binutils (ELSA-2021-4033)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-54 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-4033 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.1 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected binutils and / or binutils-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-4033.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : grub2 (ELSA-2020-5782)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-55 | During Vulnerability assessment and Penetration testing we observed that, Description of changes:  [2 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.6 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected grub2 packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-July/010163.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : yum-utils (ELSA-2018-2285)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-56 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:2285 :  An update for yum-utils is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 9.3 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected yum-utils packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-July/007913.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : nettle (ELSA-2021-1145)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-57 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-1145 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected nettle and / or nettle-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-1145.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : gupnp (ELSA-2021-2417)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-58 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-2417 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected gupnp, gupnp-devel and / or gupnp-docs packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-2417.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : rsyslog (ELSA-2022-4803)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-59 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-4803 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-4803.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : expat (ELSA-2022-6834)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-60 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-6834 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.6 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected expat, expat-devel and / or expat-static packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-6834.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : samba (ELSA-2023-1090)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-61 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-1090 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.6 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1090.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : binutils (ELSA-2018-3032)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-62 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3032 :  An update for binutils is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected binutils packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008186.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : curl (ELSA-2020-5002)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-63 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-5002 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.6 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected curl, libcurl and / or libcurl-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-5002.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : net-snmp (ELSA-2020-5350)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-64 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-5350 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-5350.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : sudo (ELSA-2021-0221)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-65 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-0221 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected sudo and / or sudo-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-0221.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2021-9395)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-66 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 6 / 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2021-9395 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-9395.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2022-9014)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-67 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2022-9014 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-9014.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : polkit (ELSA-2022-0274)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-68 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-0274 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected polkit, polkit-devel and / or polkit-docs packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-0274.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : device-mapper-multipath (ELSA-2022-7186)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-69 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-7186 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-7186.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : sudo (ELSA-2023-0291)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-70 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-0291 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected sudo and / or sudo-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-0291.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : tigervnc / and / xorg-x11-server (ELSA-2023-1594)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-71 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-1594 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1594.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Java SE Multiple Vulnerabilities (April 2023 CPU)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-72 | During Vulnerability assessment and Penetration testing we observed that, The version of Oracle (formerly Sun) Java SE or Java for Business installed on the remote host is affected by multiple vulnerabilities as referenced in the April 2023 CPU advisory:   - Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE) |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.1 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Apply the appropriate patch according to the April 2023 Oracle Critical Patch Update advisory. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://www.oracle.com/docs/tech/security-alerts/cpuapr2023cvrf.xml |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : qemu (ELSA-2023-12368)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-73 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2023-12368 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-12368.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : emacs (ELSA-2023-3481)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-74 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-3481 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-3481.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2023-12566)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-75 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2023-12566 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-12566.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : mariadb (ELSA-2018-2439)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-76 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:2439 :  An update for mariadb is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.5 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected mariadb packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-August/007941.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : dhcp (ELSA-2018-1453)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-77 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:1453 :  An update for dhcp is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.9 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected dhcp packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-May/007726.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : gnupg2 (ELSA-2018-2181)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-78 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:2181 :  An update for gnupg2 is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected gnupg2 packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-July/007879.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : sssd (ELSA-2018-3158)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-79 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3158 :  An update for sssd is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected sssd packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008201.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : glusterfs (ELSA-2018-3242)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-80 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3242 :  An update for glusterfs is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected glusterfs packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008200.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : jasper (ELSA-2018-3253)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-81 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3253 :  An update for jasper is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected jasper packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008204.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : spice (ELSA-2019-0231)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-82 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:0231 :  An update for spice is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected spice packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-January/008455.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libarchive (ELSA-2020-0203)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-83 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:0203 :  An update for libarchive is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libarchive packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-January/009540.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : unbound (ELSA-2020-2642)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-84 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2642 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:2642 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected unbound packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-June/010067.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libvpx (ELSA-2020-3876)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-85 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2020-3876 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.8 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libvpx, libvpx-devel and / or libvpx-utils packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3876.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : wpa\_supplicant (ELSA-2021-0808)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-86 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by a vulnerability as referenced in the ELSA-2021-0808 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected wpa\_supplicant package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-0808.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libldb (ELSA-2021-1072)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-87 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-1072 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-1072.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : glib2 (ELSA-2021-2147)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-88 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-2147 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-2147.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : openldap (ELSA-2022-0621)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-89 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2022-0621 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-0621.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : ntp (ELSA-2020-2663)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-90 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2663 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the RHSA-2020:2663 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected ntp packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-June/010079.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : dhcp (ELSA-2021-2357)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-91 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-2357 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 3.3 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-2357.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : rsync (ELSA-2022-6170)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-92 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by a vulnerability as referenced in the ELSA-2022-6170 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.1 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected rsync package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-6170.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : openssl (ELSA-2023-1335)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-93 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2023-1335 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.1 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1335.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2023-1904)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-94 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2023-1904 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.1 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-1904.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : cpio (ELSA-2020-3908)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-95 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by a vulnerability as referenced in the ELSA-2020-3908 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.9 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected cpio package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3908.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : dbus (ELSA-2020-4032)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-96 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4032 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 3.6 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4032.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : bluez (ELSA-2020-4001)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-97 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4001 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4001.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libcroco (ELSA-2020-4072)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-98 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4072 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libcroco and / or libcroco-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4072.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : rpm (ELSA-2021-4785)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-99 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-4785 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.1 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-4785.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : openssh (ELSA-2021-4782)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-100 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-4782 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | SSH |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-4782.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : grub2 (ELSA-2022-9469)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-101 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2022-9469 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.9 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-9469.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : bind (ELSA-2023-0402)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-102 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2023-0402 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2023-0402.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : e2fsprogs (ELSA-2020-4011)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-103 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2020-4011 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.6 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4011.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : xorg-x11-server (ELSA-2018-3410)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-104 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3410 :  An update for xorg-x11-server is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 7.2 | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected xorg-x11-server packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008225.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : spice / and / spice-gtk (ELSA-2020-4187)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-105 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4187 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4187.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : wpa\_supplicant (ELSA-2018-3107)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-106 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3107 :  An update for wpa\_supplicant is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 3.3 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected wpa\_supplicant package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008195.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : hunspell (ELSA-2020-3971)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-107 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-3971 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected hunspell and / or hunspell-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3971.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : freetype (ELSA-2020-4907)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-108 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4907 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected freetype, freetype-demos and / or freetype-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-4907.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : shim-signed (ELSA-2022-9466)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-109 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2022-9466 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected mokutil, shim-ia32 and / or shim-x64 packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-9466.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : gnutls (ELSA-2018-3050)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-110 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3050 :  An update for gnutls is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected gnutls packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008191.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : qemu-kvm (ELSA-2020-1208)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-111 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:1208 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:1208 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.8 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected qemu-kvm packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-April/009800.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : PackageKit (ELSA-2018-1224)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-112 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:1224 :  An update for PackageKit is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.1 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packagekit packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-April/007646.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libvirt (ELSA-2018-1997) (Spectre)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-113 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:1997 :  An update for libvirt is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.1 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libvirt packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-June/007819.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : systemd (ELSA-2019-0368)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-114 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:0368 :  An update for systemd is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.9 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected systemd packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-February/008492.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : tcpdump (ELSA-2019-3976)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-115 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:3976 :  An update for tcpdump is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected tcpdump package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-November/009393.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : microcode\_ctl (ELSA-2020-2432)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-116 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2432 :  The remote Redhat Enterprise Linux 7 host has a package installed that is affected by multiple vulnerabilities as referenced in the RHSA-2020:2432 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.1 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected microcode\_ctl package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-June/010061.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : dbus (ELSA-2020-2894)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-117 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2020:2894 :  The remote Redhat Enterprise Linux 7 host has packages installed that are affected by a vulnerability as referenced in the RHSA-2020:2894 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.9 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected dbus packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2020-July/010117.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : libmspack (ELSA-2020-3848)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-118 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-3848 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected libmspack and / or libmspack-devel packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-3848.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : microcode\_ctl (ELSA-2022-9507)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-119 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has a package installed that is affected by multiple vulnerabilities as referenced in the ELSA-2022-9507 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.1 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected microcode\_ctl package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2022-9507.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : setup (ELSA-2018-3249)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-120 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3249 :  An update for setup is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.6 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected setup package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008206.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : qt / and / qt5-qtbase (ELSA-2020-5021)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-121 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-5021 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2020-5021.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : krb5 (ELSA-2018-3071)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-122 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2018:3071 :  An update for krb5 is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 6.5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected krb5 packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2018-November/008189.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : openssl (ELSA-2019-0483)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-123 | During Vulnerability assessment and Penetration testing we observed that, From Red Hat Security Advisory 2019:0483 :  An update for openssl is now available for Red Hat Enterprise Linux 7 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 1.9 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected openssl packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-March/008531.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : NetworkManager (ELSA-2020-4003)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-124 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2020-4003 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://linux.oracle.com/errata/ELSA-2020-4003.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : qemu-kvm (ELSA-2021-2322)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-125 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by a vulnerability as referenced in the ELSA-2021-2322 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 3.3 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-2322.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : dnsmasq (ELSA-2021-0153)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-126 | During Vulnerability assessment and Penetration testing we observed that, The remote Oracle Linux 7 host has packages installed that are affected by multiple vulnerabilities as referenced in the ELSA-2021-0153 advisory |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 4.3 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected dnsmasq and / or dnsmasq-utils packages. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://linux.oracle.com/errata/ELSA-2021-0153.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## SSH Weak Key Exchange Algorithms Enabled

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-127 | During Vulnerability assessment and Penetration testing we observed that, The remote SSH server is configured to allow key exchange algorithms which are considered weak |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.6 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:22 | | SSH |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Contact the vendor or consult product documentation to disable the weak algorithms. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://www.nessus.org/u?b02d91cd |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Network daemons not managed by the package system

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-128 | During Vulnerability assessment and Penetration testing we observed that, Some daemon processes on the remote host are associated with programs that have been installed manually |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.1 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | |  |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Use packages supplied by the operating system vendor whenever possible.  And make sure that manual software installation agrees with your organization's acceptable use and security policies. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | |  |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## mDNS Detection (Remote Network)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-129 | During Vulnerability assessment and Penetration testing we observed that, The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 5 | Medium | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:5353 | |  |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Filter incoming traffic to UDP port 5353, if desired. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | |  |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Database Unsupported Version Detection

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-130 | During Vulnerability assessment and Penetration testing we observed that, According to its version, the installation of Oracle Database running on the remote host is no longer supported |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 10 | Critical | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Upgrade to a version of Oracle Database that is currently supported. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | http://www.nessus.org/u?ccd068d1 |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## SSH Server CBC Mode Ciphers Enabled

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-131 | During Vulnerability assessment and Penetration testing we observed that, The SSH server is configured to support Cipher Block Chaining (CBC) encryption |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
| 2.6 | Low | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:22 | | SSH |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | |  |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |

## Oracle Linux 7 : microcode\_ctl (ELSA-2019-4867)

|  |  |
| --- | --- |
| **Finding ID** | **Description** |
| ABCXYZ-132 | During Vulnerability assessment and Penetration testing we observed that, Description of changes:  [2:2 |

|  |  |  |
| --- | --- | --- |
| **CVS Score** | **Risk Rating** | **Remote Exploitability** |
|  | High | Yes |

|  |  |  |
| --- | --- | --- |
| **Affected Resource** | | **Module Name** |
| 10.101.101.176:0 | | Oracle |

|  |
| --- |
| **Security Risk** |
|  |

|  |  |
| --- | --- |
| **Business Impact** |  |

|  |
| --- |
| **Workaround / Mitigation** |
| It is recommended:  -To Update the affected microcode\_ctl package. |

|  |  |  |
| --- | --- | --- |
| **Tool used** | | **References** |
| Nessus | | https://oss.oracle.com/pipermail/el-errata/2019-December/009422.html |

|  |
| --- |
| **Proof of Concept (POC)** |
| **Figure 1** - Shows |