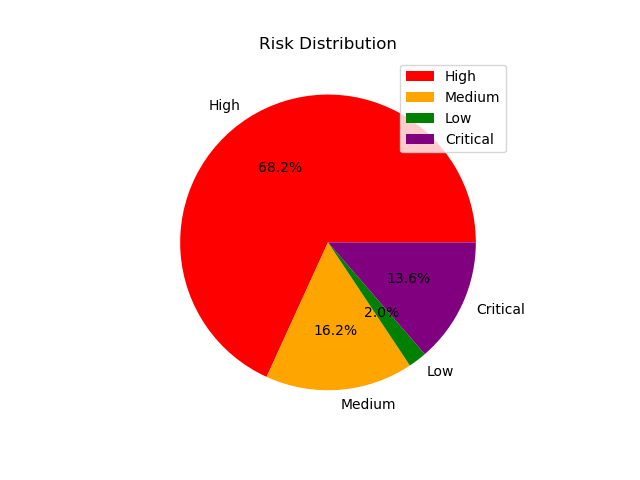
{'High': 270, 'Medium': 64, 'Critical': 54, 'Low': 8}



High Severity issues account for 270 of the total issues, Medium Severity issues account for 64 of the total issues, Low Severity issues account for 8 of the total issues, Critical Severity issues account for 54 of the total issues.

The highest risk is High with 270 issues.

The median risk is Low with 8 issues.

|  |  |
| --- | --- |
| Recommendation | Count |
| Update the affected packages. | 226 |
| Update the affected firefox package. | 52 |
| Update the affected libtiff, libtiff-devel and / or libtiff-tools packages. | 36 |
| Update the affected fribidi and / or fribidi-devel packages. | 12 |
| Update the affected freetype and / or freetype-devel packages. | 12 |
| Update the affected gdisk package. | 8 |
| Purchase or generate a proper SSL certificate for this service. | 5 |
| Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | 4 |
| Contact the vendor or consult product documentation to disable the weak algorithms. | 4 |
| Update the affected rsync and / or rsync-daemon packages. | 4 |
| Update the affected wavpack and / or wavpack-devel packages. | 4 |
| Update the affected yajl and / or yajl-devel packages. | 4 |
| Update the affected gstreamer1-plugins-good and / or gstreamer1-plugins-good-gtk packages. | 4 |
| Update the affected libxml2, libxml2-devel and / or python3-libxml2 packages. | 4 |
| Update the affected dnsmasq and / or dnsmasq-utils packages. | 4 |
| Update the affected device-mapper-multipath package. | 4 |
| Reconfigure the affected application if possible to avoid use of medium strength ciphers. | 2 |
| Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | 2 |
| Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. | 2 |
| Upgrade to Apache Log4j version 2.3.1, 2.12.3, 2.17.0 or later, or apply the vendor mitigation.  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. | 1 |
| Upgrade to Apache Log4j version 2.17.1, 2.12.4, or 2.3.2 or later, or apply the vendor mitigation.  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. | 1 |
| Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | 1 |
| Recommendation | Count |
| Update the affected packages. | 226 |
| Update the affected firefox package. | 52 |
| Update the affected libtiff, libtiff-devel and / or libtiff-tools packages. | 36 |
| Update the affected fribidi and / or fribidi-devel packages. | 12 |
| Update the affected freetype and / or freetype-devel packages. | 12 |
| Update the affected gdisk package. | 8 |
| Purchase or generate a proper SSL certificate for this service. | 5 |
| Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | 4 |
| Contact the vendor or consult product documentation to disable the weak algorithms. | 4 |
| Update the affected rsync and / or rsync-daemon packages. | 4 |
| Update the affected wavpack and / or wavpack-devel packages. | 4 |
| Update the affected yajl and / or yajl-devel packages. | 4 |
| Update the affected gstreamer1-plugins-good and / or gstreamer1-plugins-good-gtk packages. | 4 |
| Update the affected libxml2, libxml2-devel and / or python3-libxml2 packages. | 4 |
| Update the affected dnsmasq and / or dnsmasq-utils packages. | 4 |
| Update the affected device-mapper-multipath package. | 4 |
| Reconfigure the affected application if possible to avoid use of medium strength ciphers. | 2 |
| Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | 2 |
| Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. | 2 |
| Upgrade to Apache Log4j version 2.3.1, 2.12.3, 2.17.0 or later, or apply the vendor mitigation.  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. | 1 |
| Upgrade to Apache Log4j version 2.17.1, 2.12.4, or 2.3.2 or later, or apply the vendor mitigation.  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. | 1 |
| Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | 1 |

The host with the most issues is 10.1.145.41 with 103 issues.

The host with the most issues is 10.1.145.41 with 103 issues. it accounts for 26.01% of the total issues.

The host with the most issues is 10.1.145.41 with 103 issues. it accounts for 26.01% of the total issues.