Overview

Tenable Security Response Team's 2022 Threat Landscape Report is an analysis of the past year's significant vulnerabilities and mis-configurations, including major data breaches in 2022. This information provides valuable insight for organizations to ensure their security strategy and implementation align with the current threat landscape. The report highlights publicly available information on data breaches and contains references to CVE Records and CVSS Scores from critical events and key vulnerabilities that were reported and analyzed during 2022.

The 2022 Threat Landscape Report Dashboards (Tenable Vulnerability Management and Tenable Security Center) use CVE filters to display the most notable vulnerabilities, providing indicators, by vendor, for the key vulnerabilities exploited in 2022. Many of the widgets within the dashboard provide guidance to identify these vulnerabilities, including correlation between CVSSv3 scores and the CVEs discussed in the Threat Landscape Report. See the Tenable Vulnerability Management Widget Library for a comprehensive list of useful widgets. Analysts can also leverage the 2022 Threat Landscape Report Tactical Scan Template and other tactical scans for a targeted review of the infrastructure.

The Tenable 2022 Threat Landscape Report (TLR) inspects key aspects of the cybersecurity landscape and describes how organizations can revise their programs to focus on reducing risk. The TLR covers:

- Significant vulnerabilities disclosed and exploited throughout the year, including how common cloud misconfigurations can affect even large tech companies
- The continuous transformation of the ransomware ecosystem and the rise of extortion-only threat groups
- Ongoing risks, vulnerabilities and attacks within the software supply chain
- Tactics used by advanced persistent threat groups to target organizations with cyber espionage as well as financially motivated attacks.
- Breach factors and the challenges in analyzing breach data, given limited information available and lack of detailed reporting requirements
- Details of the key vulnerabilities affecting enterprise software

Use the information in this Cyber Exposure Study to perform a targeted review of your organization’s environment against the current threat and vulnerability landscape to effectively allocate resources.
The logic described in this study can be applied to any new research report, whitepaper, or applicable framework for your environment.
# 2022 Threat Landscape Retrospective Dashboard Widgets

<table>
<thead>
<tr>
<th>Widget Description</th>
<th>Widget Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>TLR 2022 - Top 5 Vulnerabilities</strong> widget features the top five vulnerabilities of 2022 as described in the [Tenable 2022 Threat Landscape Report: Log4shell, Apache Log4j - CVE-2021-44228, Follina, Microsoft Support Diagnostic Tool - CVE-2022-30190, Atlassian Confluence Server and Data Center - CVE-2022-26134, ProxyShell, Microsoft Exchange Server - CVE-2021-34473, and Known Vulnerabilities - CVE-20XX-XXXX. Vulnerabilities that match the criteria will be displayed in a bar chart, with vulnerability counts for Tenable Vulnerability Management, or an indicator matrix for Tenable Security Center.**</td>
<td><img src="image1.png" alt="Bar Chart" /></td>
</tr>
<tr>
<td>The <strong>2022 TLR Mitigated Vulnerabilities</strong> widget displays cells for the most significant vulnerabilities of 2022 that have been mitigated. Filters focus on using the CVE and Vulnerability State filters. These filters display the fixed key vulnerabilities from the 2022 Threat Landscape Report: Log4shell, Apache Log4j - CVE-2021-44228, Follina, Microsoft Support Diagnostic Tool - CVE-2022-30190, Atlassian Confluence Server and Data Center - CVE-2022-26134, ProxyShell, Microsoft Exchange Server - CVE-2021-34473, and Known Vulnerabilities - CVE-20XX-XXXX. Vulnerabilities that match the criteria will be displayed in a bar chart, with vulnerability counts for Tenable Vulnerability Management, or an indicator matrix for Tenable Security Center.**</td>
<td><img src="image2.png" alt="Indicator Matrix" /></td>
</tr>
<tr>
<td>Tenable Vulnerability Management</td>
<td><img src="image3.png" alt="Table" /></td>
</tr>
</tbody>
</table>
A fixed vulnerability is a vulnerability that was once present on a host, but is no longer present. This allows organizations to track mitigation progress and determine whether SLAs are being met. Details are provided in the Tenable 2022 Threat Landscape Report.

The 2022 TLR Key Vulnerabilities widget displays cells for the most significant vulnerabilities of 2022 using CVE filters from the 2022 Threat Landscape Report. These filters display the key vulnerabilities from 2022 as well as the notable known vulnerabilities from prior years. Details are provided in the Tenable 2022 Threat Landscape Report.

The 2022 TLR CVSS to VPR Heat Map widget provides a correlation between CVSSv3 scores and Vulnerability Priority Rating (VPR) scor-
The **2022 TLR - 90 Day Trend Analysis of Key Vulnerabilities** widget provides a 90-day analysis of the most notable vulnerabilities in 2022, leveraging the CVEs identified in the [Tenable 2022 Threat Landscape Report (TLR)](#). There are over 180 CVEs discussed in the TLR, which, combined with the trend line, helps risk managers determine how risk has been reduced over a period of 90 days.

The **2022 TLR - 90 Day Trend Analysis of Key Vulnerabilities** widget provides a 90-day analysis of the most notable vulnerabilities in 2022, leveraging the CVEs identified in the [Tenable 2022 Threat Landscape Report (TLR)](#). There are over 180 CVEs discussed in the TLR, which, combined with the trend line, helps risk managers determine how risk has been reduced over a period of 90 days.
The vulnerability last observed filter is set to 1 day to display risk changes on a daily basis.

The **2022 TLR - Mitigation Tasks** widget provides a list of patches that mitigate the key vulnerabilities in 2022, leveraging the CVEs identified in the **Tenable 2022 Threat Landscape Report (TLR)**. The Remediation Summary tool uses the concept of a Patch Chain, and identifies the top patch to remediate for the greatest risk reduction. When the top patch is applied, all other patches in the chain will be remediated.

The **2022 TLR Zero Days by Vendor** widget displays zero-day vulnerabilities directly related to the CVE contained in the **2022 Threat Landscape Report (TLR)** by vendor. For 2022, Tenable’s tracking of zero-day vulnerabilities includes flaws that were exploited in the wild, as well as flaws that were publicly disclosed prior to patches being made available or that do not have patches. Throughout 2022, as part of Tenable’s analysis of publicly available vendor advisories, disclosures and news articles, 101 zero-day vulnerabilities were identified. For contrast, Tenable identified 105 of these zero-day vulnerabilities in 2022. This represents a decrease of 4 vulnerabilities, reflecting a 3.8% drop.
<table>
<thead>
<tr>
<th>Widget Description</th>
<th>Widget Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>The 2022 TLR Zero Days by Exploit Status Available widget displays zero-day vulnerabilities directly related to the CVE contained in the 2022 Threat Landscape Report (TLR) by their exploit state. Key vulnerabilities that are exploitable are displayed by severity. For 2022, Tenable's tracking of zero-day vulnerabilities includes flaws that were exploited in the wild, as well as flaws that were publicly disclosed prior to patches being made available or that do not have patches. Throughout 2022, as part of Tenable's analysis of publicly available vendor advisories, disclosures and news articles, 101 zero-day vulnerabilities were identified. For contrast, Tenable identified 105 of these zero-day vulnerabilities in 2022. This represents a decrease of 4 vulnerabilities, reflecting a 3.8% drop. The requirements for this widget are: Tenable Vulnerability Management (Nessus).</td>
<td><img src="image1.png" alt="Zero-day vulnerabilities chart" /></td>
</tr>
</tbody>
</table>

| The 2022 TLR Zero Days by Software/Hardware Type widget displays zero-day vulnerabilities directly related to the CVE contained in the 2022 Threat Landscape Report (TLR) grouped by software/hardware type. For 2022, Tenable's tracking of zero-day vulnerabilities includes flaws that were exploited in the wild, as well as flaws that were publicly disclosed prior to patches being made available. | ![Software/hardware type chart](image2.png) |
Throughout 2022, as part of Tenable's analysis of publicly available vendor advisories, disclosures and news articles, 101 zero-day vulnerabilities were identified. For contrast, Tenable identified 105 of these zero-day vulnerabilities in 2022. This represents a decrease of 4 vulnerabilities, reflecting a 3.8% drop.
Vulnerability Landscape

The top five vulnerabilities of 2022 as described in Tenable's 2022 Threat Landscape Report:

1. Log4shell, Apache Log4j - CVE-2021-44228
2. Follina, Microsoft Support Diagnostic Tool - CVE-2022-30190
3. Atlassian Confluence Server and Data Center - CVE-2022-26134
4. ProxyShell, Microsoft Exchange Server - CVE-2021-34473
5. Known Vulnerabilities - CVE-20XX-XXXX

NOTE: Vulnerabilities are identified by their Common Vulnerabilities and Exposure (CVE) identifier. A CVE identifier consists of the letters CVE followed by the year and a sequence number (CVE-YYY-SSSSSSS). Currently, sequence numbers can be up to 7 digits in length, but are typically shorter. Both Tenable Vulnerability Management and Tenable Security Center provide a method to search for CVE identifiers using the CVE ID filter. More than a single CVE ID can be within a single CVE ID filter by separating the CVE IDs with a comma.

Additional filters can be used to narrow, or focus vulnerability results. For example, Plugin Family filters can narrow results to specific device families. Tagging can be used to group assets and tags can then be used as a filter. Date Ranges, State, Vulnerability Priority Rating (VPR), CVSS Base Scores, Exploitability Ease, and even Severity rating can be utilized to focus, narrow and refine results. More information on available filters can be found here: Tenable Vulnerability Management Vulnerability filters, Tenable Security Center Vulnerability Filters.

Specific scan templates, known as Tactical Scan Templates are pre-configured to scan for specific vulnerabilities, such as Log4Shell, ProxyLogon, and specific vulnerabilities identified by the Threat Landscape Report.
These predefined templates can be found under **Vulnerability Management → Scans → Select a Scan Template** in Tenable Vulnerability Management, or **Scans → Policies → Add a Policy** in Tenable Security Center.
Zero-Day Vulnerabilities

Zero-day vulnerabilities are a unique class of vulnerabilities because there is no patch available for them. The reason may be that the vulnerability has only recently been discovered or disclosed. Security researchers develop Proof of Concept (PoC) code to demonstrate possible vulnerabilities and disclose this information to the vendor or developer, so that a patch can be developed and tested before the vulnerability is disclosed to the general community. The window of time between when Proof of Concept code is developed and when a patch is made available is critical. System hardening limits the number of applications and services running on the system to only those that are essential, reducing the attack surface. Misconfigurations in internet-facing systems can make organizations more susceptible to attacks by providing an entry point where local exploits can be leveraged to escalate privileges. Tenable provides Compliance Audit Files, which are based on various security frameworks, including the CIS Benchmarks and DISA STIGs. Use the Policy Compliance Auditing scan template to audit the configuration of platforms running in your environment according to the appropriate framework for your environment. Results from Compliance scans can be viewed in the Host Audits Findings page in the Explore Overview.

Prioritizing with Vulnerability Priority Rating (VPR) is one approach to reduce the number of reported high risk vulnerabilities. VPR factors in the exploit code maturity, CVSSv3 impact score, vulnerability age, threat intensity, threat recency, and other threat intelligence sources. The Most Notable Vulnerabilities CVSS to VPR Heat Map (2021 Threat Landscape Retrospective) widget uses the VPR, CVSS v3 Base Score and CVE filters. Filters were created to narrow down the CVEs from the 2021 Threat Landscape Retrospective in a heat map format. The heat map highlights the Medium and High (CVSS v3 4.0-8.9) severity vulnerabilities that previously may have been ignored, that have now been reclassified as high risk based on current threat vectors. The VPR reclassification reduces the number of Critical severity (CVSS v3 9.0-10) vulnerabilities based on current threat analysis. The following group of filters is used to query vulnerabilities with a CVSS v3 Base Score of 9.0-10 and a VPR of 9.0-10 for a specific subset of CVEs. The filter values for each cell change to display results that fall into each of the ranges represented in the row and column headers.
<table>
<thead>
<tr>
<th></th>
<th>Low (VPR 0-3.9)</th>
<th>Medium (VPR 4-6.9)</th>
<th>High (VPR 7-8.9)</th>
<th>Critical (VPR 9-10)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVSSv3 (Low 0-3.9)</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>CVSSv3 (Medium 4-6.9)</strong></td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>CVSSv3 (High 7-8.9)</strong></td>
<td>0</td>
<td>3</td>
<td>29</td>
<td>25</td>
</tr>
<tr>
<td><strong>CVSSv3 (Critical 9-10)</strong></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>43</td>
</tr>
</tbody>
</table>

- **VPR is greater than or equal to** 9.0
- **VPR is less than or equal to** 10
- **CVSS v3.0 Base Score is greater than or equal to** 9.0
- **CVSS v3.0 Base Score is less than or equal to** 10
- **CVE contains** Reference the [Tenable 2022 Threat Landscape Report](#) for the most up-to-date list of CVE Identifiers.
Threat Landscape

Understanding trends from the previous year provides valuable insight into areas that organizations need to focus on in the coming year, enabling security managers to provide executive management with information to adjust the direction of the program and authorize budget. This insight also enables security analysts to audit their security infrastructure and determine the effectiveness of the infrastructure against the current threat landscape and business goals. This section provides insight and guidance into widget template creation to perform relevant queries for software supply chain and ransomware risks in an organization’s particular environment.

A custom dashboard built with widgets from the widget template feed can be exported via a schedule or manual export to PDF, CSV, or a detailed PDF. Please refer to the tenable documentation page Export a Dashboard for more details.
Key Vulnerabilities

The key vulnerabilities in the Tenable 2022 Threat Landscape Report included the most significant and highly targeted vulnerabilities published in 2022 and some that were published in prior years. The analysis of activity revealed a detailed list of key vulnerabilities that affected a wide range of vendors, which led to a surge in ransomware attacks across nearly all sectors. Vulnerabilities were identified in the following vendor products:

<table>
<thead>
<tr>
<th>Adobe</th>
<th>Amazon Web Services</th>
<th>Apache</th>
<th>Apple</th>
<th>Arm</th>
<th>Atlassian</th>
<th>Cisco</th>
<th>Citrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5</td>
<td>Fortinet</td>
<td>Google</td>
<td>GhostScript</td>
<td>Google</td>
<td>Magnitude Simba</td>
<td>Microsoft</td>
<td>Mitel</td>
</tr>
<tr>
<td>Mozilla</td>
<td>Nooie</td>
<td>Okta</td>
<td>Open Source</td>
<td>Oracle</td>
<td>Palo Alto Networks</td>
<td>Polkit</td>
<td>PTC</td>
</tr>
<tr>
<td>Pulse Secure</td>
<td>RARLAB</td>
<td>SAP</td>
<td>Solar-winds</td>
<td>SonicWall</td>
<td>Sophos</td>
<td>Trend Micro</td>
<td>VMWare</td>
</tr>
<tr>
<td>WordPres-Plugin</td>
<td>Zimbra</td>
<td>Zoho</td>
<td>Zoom</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Within the 2022 TLR, data is presented across several pie charts by vendor and software/hardware type. The same grouping is leveraged to facilitate a simple correlation between the TLR and Tenable vulnerability data in Tenable Vulnerability Management and Tenable Security Center. CVE can be viewed and grouped together into categories that make sense to organizations, for example, group all Microsoft CVEs together. Choose Select Filters, then type CVE in the window, and check the CVE box to conduct a Findings search using grouped CVE. Then enter the CVE in the search box.
Clicking on the Advanced link enables users to write out a filter manually. In the example provided below, several CVEs from the 2022 TLR are used in conjunction with a State and Last Seen filter to reduce the results to a very specific range.

The widget 2022 TLR Key Vulnerabilities displays cells for the most significant vulnerabilities of 2022 using CVE filters from the 2022 Threat Landscape Report. These filters display the key vulnerabilities from 2022 as well as the notable known vulnerabilities from prior years.
### 2022 TLR - Key Vulnerabilities

<table>
<thead>
<tr>
<th>NAME</th>
<th>SEVERITY</th>
<th>VPR</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Log4j &lt; 2.15.0 R...</td>
<td>Critical</td>
<td>10.0</td>
<td>1</td>
</tr>
<tr>
<td>Apache Log4j &lt; 2.15.0 R...</td>
<td>Critical</td>
<td>10.0</td>
<td>1</td>
</tr>
<tr>
<td>KB4601363: Windows 7...</td>
<td>Critical</td>
<td>10.0</td>
<td>1</td>
</tr>
<tr>
<td>RHEL 7 : samba (RHSA-...</td>
<td>Critical</td>
<td>10.0</td>
<td>1</td>
</tr>
<tr>
<td>KB4571719: Windows 7...</td>
<td>Critical</td>
<td>10.0</td>
<td>1</td>
</tr>
</tbody>
</table>
Learn More

Tenable Resources

Tenable 2022 Threat Landscape Report

Tenable Blog | 2022 Threat Landscape Report Tenable Vulnerability Management Dashboard

Tenable Blog | 2022 Threat Landscape Report Tenable Security Center Dashboard

Tenable Webinar | Tenable Research 2022 Recap and Defender’s Guidance for 2023

Follow Tenable’s Security Response Team on the Tenable Community

Tenable Cyber Exposure Studies

Tenable Compliance and Audit Files

Log4shell

Latest Research and Insights on CVE-2021-4428 aka Log4shell

Follina

CVE-2022-30190: Zero Click Zero Day in Microsoft Support Diagnostic Tool Exploited in the Wild

Atlassian

CVE-2022-26134: Zero-Day Vulnerability in Atlassian Confluence Server and Data Center Exploited in the Wild

Proxyshell