Tenable Cyber Exposure Study: 2021 Threat Landscape Retrospective

Last Revised: February 18, 2022
Introduction

Tenable’s 2021 Threat Landscape Retrospective is an analysis of the past year’s significant vulnerabilities and misconfigurations that led to data breaches in 2021. This information provides valuable insight for security managers and analysts 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 2021. 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 behind the Tenable.io widget and filter creation described in this study can be applied to any new research report, whitepaper, or applicable framework for your environment.

The 2021 Threat Landscape Retrospective Tenable.io Dashboard uses CVE filters to display the top five most notable vulnerabilities and provides indicators, by vendor, for the remaining key vulnerabilities identified in 2021. 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 Retrospective. See the Tenable.io Widget Library for a comprehensive list of useful widgets. Analysts can also leverage the 2021 Threat Landscape Retrospective Tactical Scan Template and other tactical scan templates for a targeted review of the infrastructure.
## 2021 Threat Landscape Retrospective Dashboard Widgets

<table>
<thead>
<tr>
<th>Widget Description</th>
<th>Widget Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Most Notable Vulnerabilities CVSS to VPR Heat Map (2021 Threat Landscape Retrospective)</strong> widget provides a correlation between CVSSv3 scores and VPR scores for the vulnerabilities associated with the CVEs discussed in Tenable’s 2021 Threat Landscape Retrospective. CVSSv3 scores are the traditional method to rate risk, while VPR is a new dynamic method based on data science analytics and threat modeling. Each cell contains a cross-mapping of CVSS and VPR scoring. The matrix uses a heat map approach where the vulnerabilities displayed in the upper-left corner have the least risk, and those displayed in the lower-right corner have the most risk. Tenable recommends mitigating risks in the lower right cells and working toward the upper left cells.</td>
<td><img src="image" alt="Heat Map" /></td>
</tr>
</tbody>
</table>
### Widget Description

The **Top 5 Vulnerabilities (2021 Threat Landscape Retrospective)** widget features the top five vulnerabilities of 2021 defined in **Tenable's 2021 Threat Landscape Retrospective**. The Cybersecurity & Infrastructure Agency (CISA) of the U.S. government issues multiple alerts over the year, citing these CVEs as some of the most favored vulnerabilities exploited by threat actors in 2021. Tenable's Security Response Team (SRT) identified the top five list of vulnerabilities to be patched as quickly as possible, factoring in CVSS scores, exploitation in the wild, government alerts, and the public availability of proof-of-concept (PoC) code.

The **Key Vulnerabilities (2021 Threat Landscape Retrospective)** widget displays cells for the most significant vulnerabilities of 2021 using the **CVE** and **Plugin Family** filters. These filters display the key vulnerabilities from 2021 as well as the notable legacy vulnerabilities from prior years. Details are provided in **Tenable's 2021 Threat Landscape Retrospective**.

<table>
<thead>
<tr>
<th>Widget Description</th>
<th>Widget Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Top 5 Vulnerabilities (2021 Threat Landscape Retrospective)</strong> widget features the top five vulnerabilities of 2021 defined in <strong>Tenable's 2021 Threat Landscape Retrospective</strong>. The Cybersecurity &amp; Infrastructure Agency (CISA) of the U.S. government issues multiple alerts over the year, citing these CVEs as some of the most favored vulnerabilities exploited by threat actors in 2021. Tenable's Security Response Team (SRT) identified the top five list of vulnerabilities to be patched as quickly as possible, factoring in CVSS scores, exploitation in the wild, government alerts, and the public availability of proof-of-concept (PoC) code.</td>
<td><img src="image1" alt="Top 5 Vulnerabilities (2021 Threat Landscape Retrospective) widget" /></td>
</tr>
<tr>
<td>The <strong>Key Vulnerabilities (2021 Threat Landscape Retrospective)</strong> widget displays cells for the most significant vulnerabilities of 2021 using the <strong>CVE</strong> and <strong>Plugin Family</strong> filters. These filters display the key vulnerabilities from 2021 as well as the notable legacy vulnerabilities from prior years. Details are provided in <strong>Tenable's 2021 Threat Landscape Retrospective</strong>.</td>
<td><img src="image2" alt="Key Vulnerabilities (2021 Threat Landscape Retrospective) widget" /></td>
</tr>
</tbody>
</table>
The **Most Notable Vulnerabilities** (2021 Threat Landscape Retrospective) widget provides a list of the most notable vulnerabilities in 2021, leveraging the CVEs identified in *Tenable's 2021 Threat Landscape Retrospective*. Tenable recommends focusing on these vulnerabilities, since Tenable Research determined they had the greatest impact during 2021.

The **Active Directory Account Related Findings** widget displays Active Directory (AD) account related findings with account totals that contain AD configuration improvement recommendations related to Kerberoasting, primary group identity, non-expiring passwords, blank passwords, weak encryption, Kerberos pre-auth, and unconstrained delegations. The plugins used in the widgets are part of the **Active Directory Starter Scan** Template and are meant to be used for preliminary analysis of AD hosts. Detailed exports are available, providing a chapter containing a table, ring chart, and iterator.
The **Mitigated Vulnerabilities (2021 Threat Landscape Retrospective)** widget provides a list of the most notable Fixed vulnerabilities in 2021, leveraging the CVEs identified in *Tenable's 2021 Threat Landscape Retrospective*. Tenable recommends focusing on these vulnerabilities, since Tenable Research determined they had the greatest impact during 2021.

<table>
<thead>
<tr>
<th>Widget Description</th>
<th>Widget Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Mitigated Vulnerabilities (2021 Threat Landscape Retrospective) widget provides a list of the most notable Fixed vulnerabilities in 2021, leveraging the CVEs identified in <em>Tenable's 2021 Threat Landscape Retrospective</em>. Tenable recommends focusing on these vulnerabilities, since Tenable Research determined they had the greatest impact during 2021.</td>
<td><img src="image" alt="Mitigated Vulnerabilities (2021 Threat Landscape Retrospective)" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PLUG ID</th>
<th>NAME</th>
<th>SEVERITY</th>
<th>CVSS TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>100899</td>
<td>Google Chrome &lt; 90.0.4432.116 Multiple Vulnerabilities</td>
<td>Critical</td>
<td>1</td>
</tr>
<tr>
<td>100898</td>
<td>Security Updates for Microsoft Office Products (November 2021)</td>
<td>High</td>
<td>13</td>
</tr>
<tr>
<td>100897</td>
<td>Security Updates for Microsoft Excel (November 2021)</td>
<td>High</td>
<td>12</td>
</tr>
<tr>
<td>100896</td>
<td>Google Chrome &lt; 90.0.4432.116 Multiple Vulnerabilities</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>100893</td>
<td>KB404129 - Windows 7 and Windows Server 2008 R2 Security Update (01/17/2019)</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>100892</td>
<td>KB404134 - Windows 10 Version 1803 and Windows Server 2016 Security Update Cumulative</td>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>100891</td>
<td>KB404127 - Windows 10 Version 1803 and Windows Server 2016 Security Update Cumulative</td>
<td>High</td>
<td>6</td>
</tr>
<tr>
<td>100890</td>
<td>Google Chrome &lt; 90.0.4432.116 Multiple Vulnerabilities</td>
<td>High</td>
<td>2</td>
</tr>
<tr>
<td>100889</td>
<td>Google Chrome &lt; 90.0.4432.116 Multiple Vulnerabilities</td>
<td>Critical</td>
<td>1</td>
</tr>
<tr>
<td>100888</td>
<td>KB405515 - Windows 7 and Windows Server 2008 R2 Security Update Cumulative</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>100887</td>
<td>KB405574 - Windows 10 Version 1607 and Windows Server 2016 Security Update Cumulative</td>
<td>High</td>
<td>2</td>
</tr>
</tbody>
</table>
Vulnerability Landscape

Many of the critical vulnerabilities disclosed in 2021 do not apply to every environment. For example, in March, Microsoft disclosed a state-sponsored cyberespionage campaign that exploited four zero-day vulnerabilities in Microsoft Exchange Server that had begun in January. Organizations that were not running a Microsoft Exchange Server did not need to be concerned about this disclosure. This section provides insight and guidance into widget template creation to perform relevant queries for the software and systems running in an organization’s particular environment.
ProxyLogon and PrintNightmare

The ProxyLogon and PrintNightmare vulnerabilities were the top two vulnerabilities of 2021 identified in the Threat Landscape Retrospective. The CVE filter is the only filter used for each vulnerability in the Top 5 Vulnerabilities (2021 Threat Landscape Retrospective) widget. Use the CVE filter rather than the plugin ID filter to ensure that when new plugins associated with the CVE are released, results will be displayed for all vulnerabilities associated with the CVE. Tenable’s CVE search page lists all existing plugins associated with each CVE.

- ProxyLogon filter: **CVE contains CVE-2021-26855**
- PrintNightmare filter: **CVE contains CVE-2021-34527**

**Tactical scan templates**, such as the ProxyLogon: MS Exchange and PrintNightmare scan templates can be used to run targeted scans that detect specific vulnerabilities. Users also have the option to create custom scans using the Advanced Scan Template with specific plugins enabled, if a scan template does not exist for CVEs of particular interest in their environment.

The Tenable.io Widget Library also contains widget templates for ProxyLogon and PrintNightmare, as shown below.
See the Learn More section of this Cyber Exposure Study for more Tenable resources on ProxyLogon and PrintNightmare.
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>CVSSv3 4.0 - 6.9</th>
<th>VPR 0.0-3.9</th>
<th>VPR 4.0-6.9</th>
<th>VPR 7.0-8.9</th>
<th>VPR 9.0-10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>CVSSv3 7.0 - 8.9</td>
<td>0</td>
<td>3</td>
<td>10</td>
<td>148</td>
</tr>
<tr>
<td>CVSSv3 9.0 - 10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>57</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:
Expand to view or copy the CVEs from the 2021 Threat Landscape Retrospective

Emerging Flaws in Legacy Software

One of the top two vulnerabilities of 2021 was PrintNightmare, a vulnerability in the Windows Print Spooler. Print Spooler was a feature that was used for many years to share printers that had to be connected via a Line Printer port to a computer. These ports have not been used in many years, but the service was still enabled by default and was ignored until someone discovered that it could be exploited. The immediate fix for PrintNightmare was to disable the services. The plugin for PrintNightmare checks whether the services are enabled. Many exploits for older, well-established software have led to significant data breaches.

Organizations can be blindsided by a vulnerability in 25-year-old software that is now used throughout most of the Internet. Determined attackers often spend years gathering intelligence on a target's network before striking in a big way. Tenable provides tactical scan templates and widget templates for many well-known legacy vulnerabilities.

Vulnerabilities and Misconfigurations

Embedded devices are known to leverage shared libraries and third party code and as a result may be affected by the vulnerabilities and misconfigurations in the list below. The 2021 Threat Landscape Retrospective Tenable.io dashboard identifies vulnerabilities to enable users to proactively mitigate any risk for sensitive control systems or Operational Technology (OT). Tenable.ot can detect flaws that lead to exploitation of the vulnerabilities across libraries and Software Development Kits (SDKs) found in billions of OT devices.

- URGENT/11
- Ripple20
- AMNESIA:33
- NUMBER:JACK
- NAME:WRECK
- NUCLEUS:13
- INFRA:HALT
- BadAlloc
Security standards, such as PCI DSS and NIST require organizations to manage a system development life cycle that includes software updates, but it is not always possible to update embedded devices.
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, as shown below.
Software Supply Chain

The software supply chain is a major source of risk, especially since so many modern devices run some form of software. The COVID-19 pandemic accelerated migration to remote work and cloud computing, which made network devices an attractive target for attackers. For example, Secure Socket Layer Virtual Private Networks (SSL VPNs) were heavily targeted in 2021 even though the vulnerabilities were published in 2020 or earlier. VPN vulnerabilities have been very popular with ransomware groups, since they provide an entry point for attackers to gain access to the network. Ransomware groups leveraged legacy VPN vulnerabilities in Citrix, Fortinet, and Pulse Secure. In addition to these legacy flaws, attackers used zero-days in SonicWall and Kaseya to gain entry into targeted networks to deploy ransomware, or in the case of the Accellion flaws, to exfiltrate sensitive files.

Organizations were faced with higher risks from interdependencies of software libraries. Attacks on the software supply chain caused major disruption in the form of breaches and ransomware attacks. Third party software libraries that are embedded in applications can put an organization at risk. The more pervasive the library, the more likely there will be attempts to exploit it. Tenable’s 2021 Threat Landscape Retrospective provides valuable lessons learned as attackers relentlessly exploited the software supply chain. Software supply chain attacks were a key feature of the report. Open source libraries and repositories were compromised. Vulnerabilities in Log4j, a Java logging library used by hundreds of applications and services, is a prime example of how much impact one library can have.

The log4shell - High Risk Vulnerabilities: Apache, Log4j, and Java and log4shell - Log4j Concerns widgets shown below display how Tenable examined the software supply chain by using CPEs for an explicitly known problem. Tenable used the CPE strings in the widget template queries, since initial reports about the vulnerabilities contained information about certain Java Development Kits (JDKs) and other issues related to Log4j.
Tenable has provided the log4shell Critical Vulnerability dashboard template in Tenable.io. The Log4Shell, Log4Shell Remote Checks, and Log4Shell Vulnerability Ecosystem tactical scan templates are also available. A list of Tenable plugins to identify these vulnerabilities can be found on the Tenable Plugins Page.

The CPE filter can be used to create custom widgets or workbench searches for critical software that is part of your organization’s supply chain. The log4Shell - Log4j Concerns widget uses the following filters for the Java Detection (JRE/JDK) Vulnerabilities Identified cell.

- CPE contains java, jre, jdk
- Severity is equal to Info, Low, Medium, High, Critical

Note: There are many Info severity plugins that contain useful information. The Info severity filter must be used to display plugins with an Info severity in dashboards and widgets. The filter used in the following image displays results for all severities, including Info.

The log4Shell - Log4j Concerns widget uses the following filters for the Log4j (Installed) Vulnerabilities Identified cell.

- CPE contains log4j
- Severity is equal to Info, Low, Medium, High, Critical
A search filter interface with the following options:

- **Filters**
- **By Plugin**
- **By Asset**

**Search** field with a filter query. The filter conditions are as follows:

1. **OP:**
   - Contains
   - Is equal to

2. **Severity:**
   - Info
   - Low
   - Medium
   - High
   - Critical

**Saved Searches** dropdown menu.

**Apply** button to apply the filters, **Reset Filters** button to reset all filters, and **Cancel** button to close the interface.
Ransomware

Ransomware attacks that use Active Directory (AD) to propagate or perform reconnaissance require privileged access to the directory. Many organizations do not properly restrict or manage the use of privileged AD accounts, leaving systems exposed to ransomware and other types of attacks. Ensure that AD does not contain critical misconfigurations that allow attackers to deploy payloads through vulnerable systems.

- The Active Directory Account Related Findings widget in Tenable.io uses the Plugin ID filter for the account-related plugins contained in the Active Directory Starter Scan template: 150483, 150481, 150487, 150480, 150482, 150489, 150485.

- The Active Directory Vulnerabilities (Kerberos, Trust Relationships, Null Sessions) widget uses the Plugin ID filter for the vulnerability-related plugins contained in the Active Directory Starter Scan template: 150488, 150484, 150486.

- The Microsoft Active Directory Findings widget uses the CPE contains microsoft:active_directory filter to display all plugins that match the CPE.

- All three widgets use the Severity filter for Info, Low, Medium, High, and Critical to ensure that Info plugins are displayed. The image below displays a couple Info Severity plugins for AD.

For information about how to identify AD exposures, see the AD section of the Ransomware Tenable Cyber Exposure Study and the Active Directory is Now in the Ransomware Crosshairs Tenable Blog.
Key Vulnerabilities

The key vulnerabilities in the 2021 Threat Landscape Retrospective included the most significant and highly targeted vulnerabilities published in 2021 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 vendors’ products:

<table>
<thead>
<tr>
<th>Accellion</th>
<th>Adobe</th>
<th>Apache</th>
<th>Apple</th>
<th>Arm</th>
<th>BQE</th>
<th>Cisco</th>
<th>Confluence</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5</td>
<td>FatPipe</td>
<td>Fortinet</td>
<td>GhostScript</td>
<td>Google</td>
<td>Ivanti</td>
<td>Kaseyana</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Realtek</td>
<td>RedHat</td>
<td>Qualcomm</td>
<td>Solarwinds</td>
<td>SonicWall</td>
<td>Swisslog</td>
<td>Healthcare</td>
<td>Vmware</td>
</tr>
</tbody>
</table>

**OpenSource**: Discourse, DNSMASQ, EXIM, Grub2, LinuxK Kernel, OpenSSL, Sudo, WebSVN

**Protocols, Stacks, and Software Development Kits (SDKs)**: BadAlloc, Domain Name Server Ecosystem, Eltima SDK, INFRA:HALT, NAME:WRECK, NUCLEUS:13, NUMBER:JACK

![Key Vulnerabilities (2021 Threat Landscape Retrospective)](image)
Analysis was performed during the creation of the Key Vulnerabilities (2021 Threat Landscape Retrospective) widget to determine the best way to display the key vulnerabilities from 2021, which included legacy vulnerabilities from prior years. In this case, a Vulnerability Published filter for Jan 1, 2021 to December 31, 2021 would not have included the highly targeted legacy vulnerabilities from the years prior to 2021. A better approach was to use the CVE and Plugin Family filters together, as shown below. These filters grouped the CVEs with their respective operating systems and included the key vulnerabilities from the years prior to 2021.
Learn More

Tenable Resources

Tenable Blog | Threat Landscape Retrospective
Tenable Blog | 2021 Threat Landscape Retrospective Tenable.io Dashboard
Tenable Webinar | Tenable Research 2021 Recap and Defender’s Guidance for 2022

Follow Tenable’s Security Response Team on the Tenable Community

Tenable’s 2021 Threat Landscape Retrospective Report
Tenable Compliance and Audit Files
Tenable Cyber Exposure Studies

PrintNightmare

Tenable Blog | Microsoft Releases Out-of-Band Patch for PrintNightmare Vulnerability in Windows Print Spooler
Tenable Blog | The PrintNightmare Continues: Another Zero-Day in Print Spooler Awaits Patch
Tenable Blog | Proof-of-Concept Leaked for Critical Windows Print Spooler Vulnerability

Active Directory

Tenable Blog | How to Protect Active Directory Against Ransomware Attacks
Tenable Cyber Exposure Study: Ransomware

External Resources

Atlantic Trust | Breaking trust: Shades of crisis across an insecure software supply chain
CISA | Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
CISA | Software Supply Chain Attacks Technical Reference
CISA | Stop Ransomware
CISA | Alerts