Tenable Cyber Exposure Study - Defending Against Ransomware

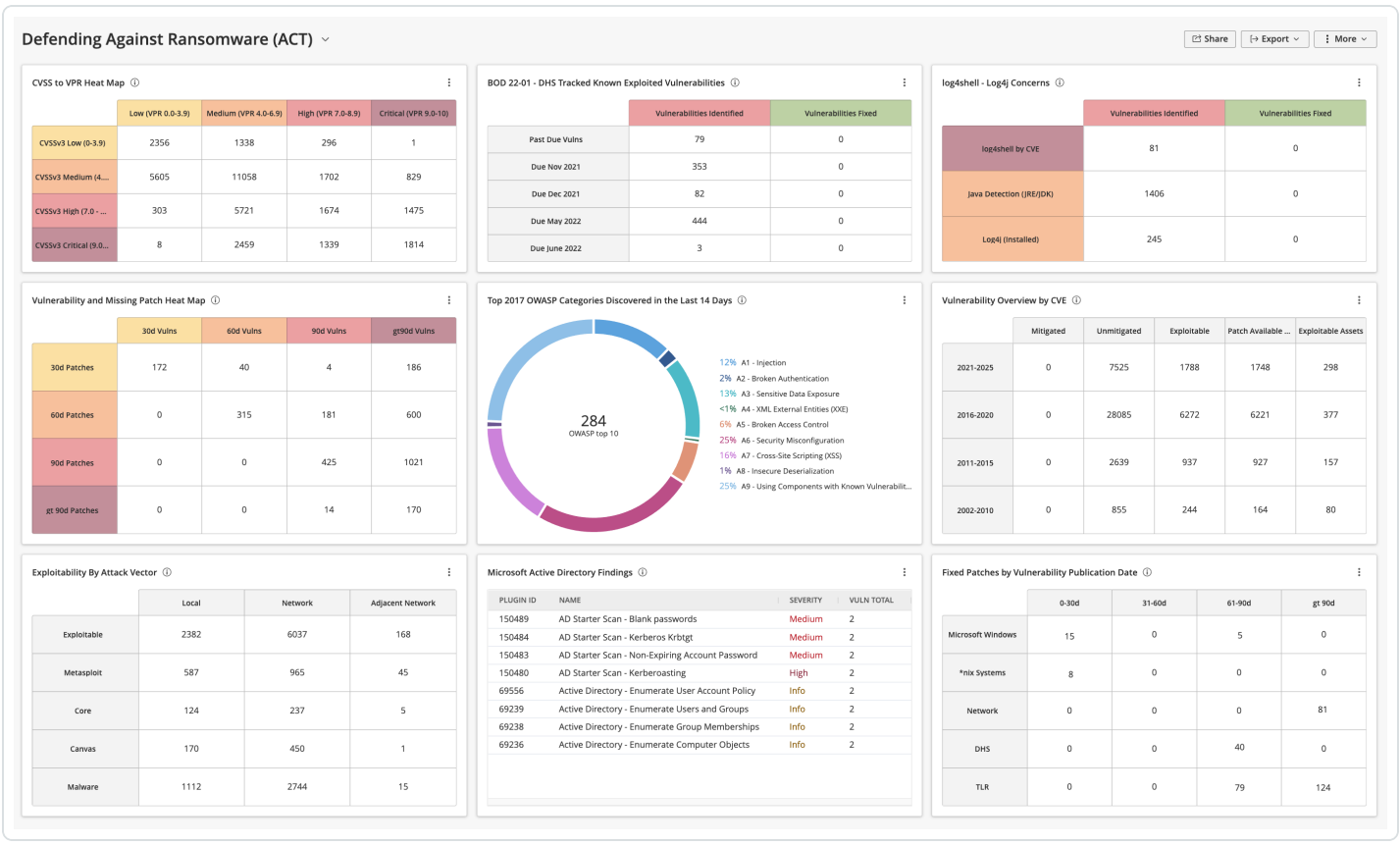
Last Revised: July 06, 2022

Table of Contents

Introduction

Ransomware attacks leverage well-known and established software vulnerabilities and poor cyber hygiene. Successful ransomware attacks can cripple an organization with increased costs and lost revenue. There are many contributing factors to the upward trend of ransomware. The most important is the large number of software vulnerabilities and misconfigurations, along with Active Directory (AD) weaknesses that enable attackers to escalate privileges. Threat actors leverage poor cyber hygiene to their advantage to gain a foothold and propagate attacks. Ransomware has been very profitable for organized crime, which targets lucrative businesses that can afford large payouts. Many organizations purchase ransomware insurance to mitigate the cost of a breach, but insurers are starting to push back against large payouts if the organization is found to be negligent in following industry security guidance.

Ransomware is a symptom of poor cyber hygiene and security awareness, which can impact operational availability and lead to increased cost. Comprehensive and regularly tested Disaster Recovery and Data Recovery plans go a long way toward combating the effects of ransomware and other threats to the business. The Defending Against Ransomware (ACT) Tenable.io Dashboard provides an in-depth focus on cyber hygiene, enabling IT staff to identify vulnerabilities that would have the most impact to the organization during a ransomware attack.



Defending Against Ransomware (ACT)

Share | Export | More

CVSS to VPR Heat Map

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	2356	1338	296	1
CVSSv3 Medium (4....	5605	11058	1702	829
CVSSv3 High (7.0 - ...	303	5721	1674	1475
CVSSv3 Critical (9.0...	8	2459	1339	1814

BOD 22-01 - DHS Tracked Known Exploited Vulnerabilities

	Vulnerabilities Identified	Vulnerabilities Fixed
Past Due Vulns	79	0
Due Nov 2021	353	0
Due Dec 2021	82	0
Due May 2022	444	0
Due June 2022	3	0

log4shell - Log4j Concerns

	Vulnerabilities Identified	Vulnerabilities Fixed
log4shell by CVE	81	0
Java Detection (JRE/JDK)	1406	0
Log4j (Installed)	245	0

Vulnerability and Missing Patch Heat Map

	30d Vulns	60d Vulns	90d Vulns	gt90d Vulns
30d Patches	172	40	4	186
60d Patches	0	315	181	600
90d Patches	0	0	425	1021
gt 90d Patches	0	0	14	170

Top 2017 OWASP Categories Discovered in the Last 14 Days

12% A1 - Injection
2% A2 - Broken Authentication
13% A3 - Sensitive Data Exposure
<1% A4 - XML External Entities (XXE)
6% A5 - Broken Access Control
25% A6 - Security Misconfiguration
16% A7 - Cross-Site Scripting (XSS)
1% A8 - Insecure Deserialization
25% A9 - Using Components with Known Vulnerabilit...

Vulnerability Overview by CVE

	Mitigated	Unmitigated	Exploitable	Patch Available ...	Exploitable Assets
2021-2025	0	7525	1788	1748	298
2016-2020	0	28085	6272	6221	377
2011-2015	0	2639	937	927	157
2002-2010	0	855	244	164	80

Exploitability By Attack Vector

	Local	Network	Adjacent Network
Exploitable	2382	6037	168
Metasploit	587	965	45
Core	124	237	5
Canvas	170	450	1
Malware	1112	2744	15

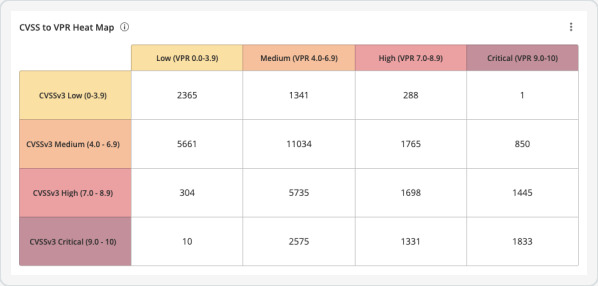
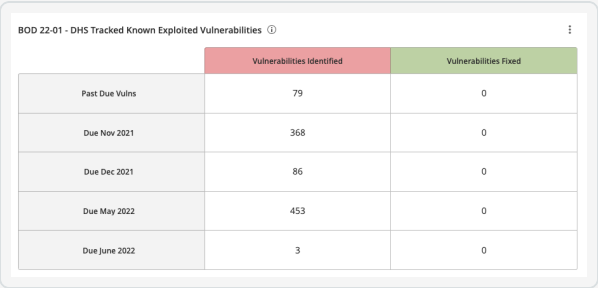
Microsoft Active Directory Findings

PLUGIN ID	NAME	SEVERITY	VULN TOTAL
150489	AD Starter Scan - Blank passwords	Medium	2
150484	AD Starter Scan - Kerberos Krbtgt	Medium	2
150483	AD Starter Scan - Non-Expiring Account Password	Medium	2
150480	AD Starter Scan - Kerberoasting	High	2
69556	Active Directory - Enumerate User Account Policy	Info	2
69239	Active Directory - Enumerate Users and Groups	Info	2
69238	Active Directory - Enumerate Group Memberships	Info	2
69236	Active Directory - Enumerate Computer Objects	Info	2

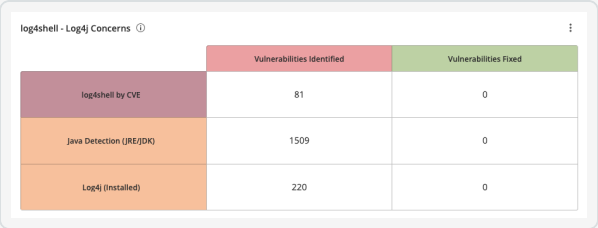
Fixed Patches by Vulnerability Publication Date

	0-30d	31-60d	61-90d	gt 90d
Microsoft Windows	15	0	5	0
*nix Systems	8	0	0	0
Network	0	0	0	81
DHS	0	0	40	0
TLR	0	0	79	124

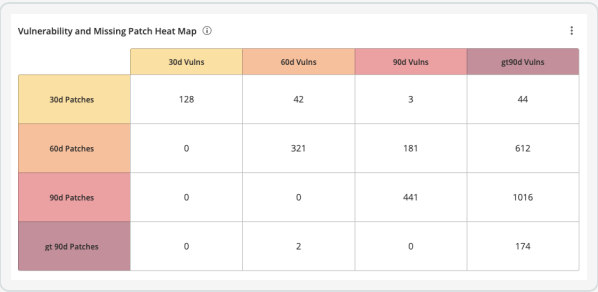
Defending Against Ransomware (ACT) Dashboard Widgets

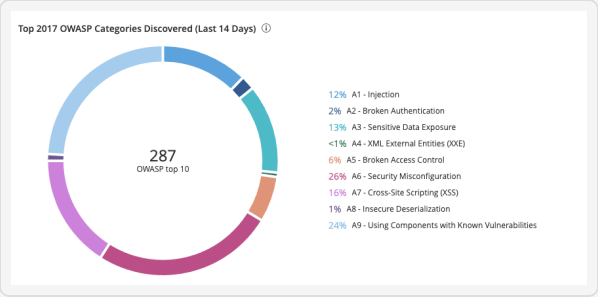
Widget Description	Widget Image
The *CVSS to VPR Heat Map* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, provides a correlation between CVSSv3 scores and VPR scores for the vulnerabilities present in the organization. Each cell consists of a cross-mapping of CVSS & VPR scores. The widget uses a heat map approach, with the upper left corner containing the vulnerabilities with the lowest risk. Moving lower and to the right in the matrix, the colors change from yellow to red as the risk levels increase. Tenable recommends mitigating risks shown in the lower right cells and working towards the upper left cells, since the lower right cells represent the highest risk.	
The *BOD 22-01 - DHS Tracked Known Exploited Vulnerabilities* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and the Tenable.io widget library, displays vulnerabilities derived from the CISA Known Exploited Vulnerabilities Catalog. The widget uses the *CVE* filter to exactly match the *Active* and *Fixed* vulnerabilities that match the CVEs included in the CISA Known Exploited Vulnerabilities Catalog. For more information, please see the full Binding Operational Directive 22-01.	

The *log4shell - Log4j Concerns* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and the Tenable.io widget library, uses the *Vulnerability State* filter with the *CVE* filter to display *Active* and *Fixed* Log4j and Java vulnerabilities. This matrix alerts organizations to potential concerns regarding the Log4j vulnerability. Displayed are the vulnerabilities that are directly associated with the log4shell CVEs: *CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-4104, and CVE-2021-45105*, and Log4j installations. Since installing Java v8 is also a requirement to address this exploit, a row of vulnerabilities that are associated with Java, JRE, and JDK is displayed.



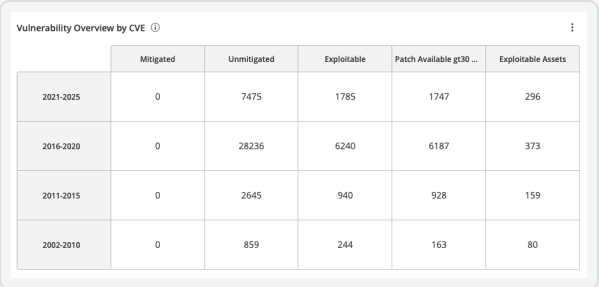
The *Vulnerability and Missing Patch Heat Map* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, uses the *Vulnerability Published* date filter cross mapped with the *Patch Published* date filter to show the organization's current vulnerability state. The *Patch Published* dates indicate when a vendor published a patch for the vulnerability, while the *Vulnerability Published* date is the date when the vulnerability was first published (for example, the date the CVE was published to NVD). Each cell consists of a cross-mapping of Patch Publication and Vulnerability Public-



ation. The widget uses a heat map approach, with the upper left corner containing the vulnerabilities and patches that have been published in the last 30 days. Moving lower and to the right in the matrix, the colors change from yellow to red as the risk levels increase. Tenable recommends mitigating risks shown in the lower right cells and working towards the upper left cells, since the lower right cells represent missing patches associated with vulnerabilities that have been present within the organization for a longer time period. Vulnerabilities displayed in this table are based on the plugins in the Local Security Checks plugin families for each Operating System. Tenable provides a comprehensive collection of plugins for a large variety of operating systems to check for security issues, which are enumerated on the Tenable Plugins Page.	
The *Top 2017 OWASP Categories Discovered in the Last 14 days* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays the percentages of active Web Application vulnerabilities from Tenable.io WAS by OWASP category.	

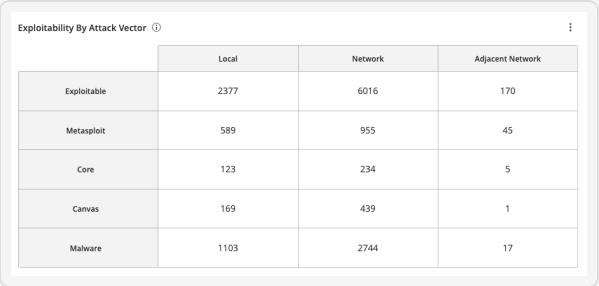
The *Vulnerability Overview by CVE* Widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays a count of the following:

- Mitigated (**Fixed**) Vulnerabilities
- Unmitigated (**New, Active,** or **Resurfaced**) vulnerabilities
- Exploitable vulnerabilities
- Vulnerabilities with a patch available
- Vulnerabilities with an exploit available



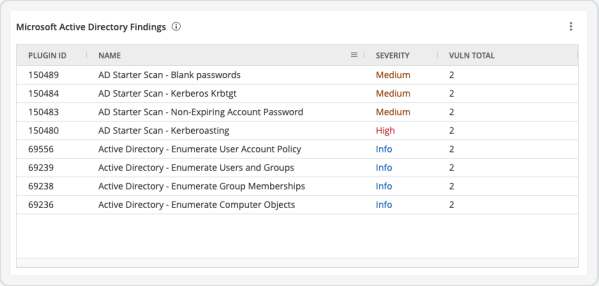
	Mitigated	Unmitigated	Exploitable	Patch Available gt30 ...	Exploitable Assets
2021-2025	0	7475	1785	1747	296
2016-2020	0	28236	6240	6187	373
2011-2015	0	2645	940	928	159
2002-2010	0	859	244	163	80

The *Exploitability By Attack Vector* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays exploitable vulnerabilities by the CVSS Exploitability Metric Vectors: **AV:N (Network), AV:A (Adjacent Network),** and **AV:L (Local)**. There is a row for each exploit framework. The CVSS metric vector specifies if the vulnerability is locally or remotely exploitable. The description for "Attack Vector" can be found in the First.org CVSS Specification Document.



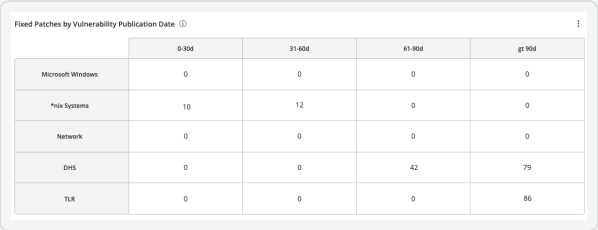
	Local	Network	Adjacent Network
Exploitable	2377	6016	170
Metasploit	589	955	45
Core	123	234	5
Canvas	169	439	1
Malware	1103	2744	17

The *Microsoft Active Directory Findings* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays Active Directory vulnerabilities using the CPE filter for *cpe:/a:microsoft:active_directory*.



PLUGIN ID	NAME	SEVERITY	VULN TOTAL
150489	AD Starter Scan - Blank passwords	Medium	2
150484	AD Starter Scan - Kerberos Krbtgt	Medium	2
150483	AD Starter Scan - Non-Expiring Account Password	Medium	2
150480	AD Starter Scan - Kerberoasting	High	2
69556	Active Directory - Enumerate User Account Policy	Info	2
69239	Active Directory - Enumerate Users and Groups	Info	2
69238	Active Directory - Enumerate Group Memberships	Info	2
69236	Active Directory - Enumerate Computer Objects	Info	2

The *Fixed Patches by Vulnerability Publication Date* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays counts of fixed vulnerabilities grouped by the patch publication date. This matrix assists organizations with mapping mitigation progress and presents data to determine whether organizational SLAs are being met. Each cell contains a count of fixed vulnerabilities grouped by Microsoft Windows systems, *nix systems, Network devices, and vulnerabilities specified in the DHS BOD 22-01 and Tenable's 2021 Threat Landscape Retrospective with a patches published 0-30, 31-60, 61-90, and more than 90 days ago.


Fixed Patches by Vulnerability Publication Date

	0-30d	31-60d	61-90d	gt 90d
Microsoft Windows	0	0	0	0
*nix Systems	10	12	0	0
Network	0	0	0	0
DHS	0	0	42	79
TLR	0	0	0	86

Common Exploits

Attackers prey on remote access infrastructure and web application flaws for entry points into the network. Vulnerabilities are exposures that can be exploited and can be in the form of a software defect, configuration error, or basic human error. Ransomware strains are increasingly using software vulnerabilities as the initial attack vector, with ransomware groups targeting Oracle WebLogic (CVE-2019-2729) and Pulse Secure (CVE-2019-11510) vulnerabilities. These flaws tend to be older and well known, so it is essential to continuously assess the entire attack surface as the environment changes and new vulnerabilities appear – especially web applications, remote access infrastructure, and Operational Technology (OT).

As information about new vulnerabilities is discovered and released into the public domain, Tenable Research designs programs to detect them. Each plugin contains vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue. Tenable Research has published over 165,000 plugins, which can be found on the Tenable Plugins Page.

Zero-Days

Zero-day vulnerabilities are a unique class of vulnerabilities because there is no patch available for them. Organizations, both benign and malicious, strive to keep knowledge of zero-day vulnerabilities private: the former, so they can be more easily exploited, and the latter to buy time until a patch is developed and tested. The tricky part is when a zero-day vulnerability becomes public before a patch is available, triggering a mad scramble for malicious attackers to exploit the vulnerability while security professionals research, test, and deploy patches and mitigation on the fly, such as an IPS signature. Vulnerabilities in widely used libraries, such as log4j and Apache Struts, present a larger nightmare, since these libraries are used by many applications that all must be patched and tested before deployment. Commonly, zero-day patches are updated as more information about the vulnerability is discovered. Once patches or mitigation are put in place, Nessus can be run with the appropriate plugins to verify that the vulnerability is not available for remote exploitation.

Read Tenable's coverage of Log4j and Apache Struts for more information about these serious vulnerabilities.

Headline Attacks

While the release of a zero-day vulnerability certainly causes headlines, there are other attacks that generate a news frenzy because of their impact. Such headline attacks can cause headaches for harried security professionals who must repeatedly report to management and third parties where the organization stands in relation to the attack. The good news is that organizations that keep up-to-date with patching and mitigation can produce dashboards that demonstrate readiness for such an attack.

Kaseya VSA

On July 2, 2021, MSPs using Kaseya Virtual System Administrator (VSA) were targeted by a coordinated ransomware attack attributed to REvil, one of the world's most active Ransomware-as-a-Service (RaaS) groups. Tenable's Security Response Team (SRT) published a blog post regarding this attack, which can be viewed here: CVE-2021-30116: Multiple Zero-Day Vulnerabilities in Kaseya VSA Exploited to Distribute REvil Ransomware. Tenable has released plugins that will detect the presence of Kaseya VSA and the Kaseya Agent for Windows, as well as Indicators of Compromise (IoCs) that relate to the Kaseya ransomware attack.

Plugin ID	Plugin Name	Type	Severity
151371	Kaseya Agent Installed (Windows)	Local	Informational
151372	Kaseya Virtual System Administrator (VSA) Detection	Remote	Informational
151424*	Potential exposure to Kaseya VSA ransomware attack	Local	Critical

*Plugin 151424: *Potential exposure to Kaseya VSA ransomware attack* detects the potential presence of agent.exe or agent.crt IoCs on remote host machines. This can indicate that the host might have been targeted in the Kaseya VSA ransomware attack. Tenable strongly recommends manually verifying the results and taking appropriate remediation actions, if the compromise is confirmed.

For more information about displaying and tracking common exploits in the environment, see the Defending Against Ransomware (ACT) Dashboard Widget explanations.

Most Targeted Attack Vectors

Attackers typically target open services with known vulnerabilities, since those are the easiest to exploit. The Center for Internet Security (CIS) develops benchmarks for numerous operating systems and devices, which provide guidance for hardening systems by turning off any services that are not required for the system to perform its function. This is particularly important for services that are shipped with the operating system but are no longer supported, such as Adobe Flash or Microsoft Internet Explorer. Exploit kits are usually designed for easy targets, such as vulnerable services. Sophisticated attackers are capable of exploiting zero-day vulnerabilities, but usually look for easy targets first.

Ransomware attacks may vary in technique, depending on the sophistication of the attacker, but typically the same general script is followed:

1. Attackers gain access via a known flaw, which may exist in:
    - Unpatched devices (exploitation)
    - New or unknown devices (exploitation)
    - Poorly configured devices (exploitation)
    - Phishing (emails, attachments, Dropbox)
    - Credential Stuffing (web site attacks, RDP)
    - Web Shell/Loader (web site attacks, php, perl, python, asp, etc.)
2. Attackers disable key services and scrub log entries, moving laterally through the network to gain a foothold by mapping the network and compromising assets beyond the original attack. Cobalt Strike, originally released as a penetration testing tool, is the most common tool used. Versions that have been cracked are widely distributed in hacking forums. Cobalt Strike is loaded into memory via DLL hijacking. Once loaded, many native operating system commands can be run, such as: net, ping, whoami, wmic, and many more that help the attacker evade detection. Other tools, commonly scripts, are used to disable security programs.
3. Attackers gain privileged access to the Active Directory (AD) Domain. Programs such as Mimikatz and Bloodhound are commonly used to retrieve information from other assets to gain access to the AD Controller.

4. Attackers leverage escalated privileges to install code throughout the environment. Once an attacker gains privileged access, there is little that can be done. As access is gained into other devices, additional Cobalt Strike Beacons execute PowerShell scripts, log keystrokes, take screenshots, download files, and spawn other payloads. The Windows Management Instrumentation Command-Line (WMIC), and PowerShell are commonly used to execute files pushed via Server Message Block (SMB) to other assets. Attackers commonly perform file searches for key terms such as “policy,” “bank,” “2021,” “statement,” and “insurance,” looking for financial documents and documents that contain accounting information.

5. Attackers commonly search for backups that are accessible from the network to prevent their targets from restoring data and will typically encrypt one or two systems as a test to ensure they will be successful.

6. Attackers exfiltrate data with programs such as, Rclone, WinSCP, StealBIT, and MegaSYNC and subsequently encrypt data, which disrupts operations. All the remaining systems are encrypted using PsExec to execute the malware after the malware is pushed via SMB. Microsoft Group Policy (GPO) is also used to push the malware to the Domain Controller. Microsoft’s System Center Configuration Manager (SCCM) or Remote Monitoring and Management (RMM) is also commonly used to push malware. Attackers will typically delete the Volume Shadow Copy Service (VSS) and associated files to prevent restoration.

Vulnerabilities

Vulnerabilities are exposures that can be exploited and can be in the form of a software defect, configuration error, or basic human error. The impact of exploiting a vulnerability depends on the value of the targeted asset. Risk Based Vulnerability Management (RBVM) is a process that reduces vulnerabilities across the attack surface by prioritizing remediation based on the risks posed to the organization. Unlike legacy vulnerability management, RBVM goes beyond discovering vulnerabilities by providing threat context and insight into potential business impact.

Identification

As information about new vulnerabilities is discovered and released into the public domain, Tenable Research designs programs to detect them. Each plugin contains vulnerability information, a simplified set of remediation actions, and the algorithm to test for the presence of the security issue. Tenable Research has published over 165,000 plugins, which can be found on the Tenable Plugins Page.

Prioritize Vulnerability Scanning

Identifying vulnerabilities and configuration errors in the infrastructure is the first step to determine susceptibility to ransomware attacks. Prioritize vulnerability scanning by targeting critical assets first. Create Tactical Scan Policies and leverage scan templates to ensure scans are configured appropriately for the assets' function, such as:

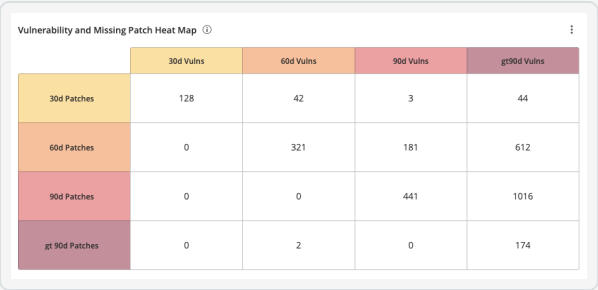
- Critical business servers
- Critical infrastructure devices
- Managed servers
- User / Desktop
- Off-site (VPN, Managed)
- Production servers
- Development servers

- Test systems
- Web servers
- Operational Technology devices

Organizations often define a “gold standard” for various system deployments, based on the CIS benchmarks. However, day-to-day operational requirements tend to cause a drift from this standard over time, creating weak links. Technical staff can use the Tenable.io Cyber Exposure Platform to analyze endpoint operating systems, software configurations, web applications, and Operational Technology (OT) devices. Organizations can verify that established configuration policies are followed by including Tenable CIS Audits in policy compliance vulnerability scans. Use Tenable.io to configure vulnerability, compliance, and web application scans. Assessing the configuration of systems within the network is a vital step in risk-based vulnerability management (RBVM).

Determine Current State

The *Vulnerability and Missing Patch Heat Map* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, uses the *Vulnerability Published* date filter cross mapped with the *Patch Published* date filter to show the organization's current vulnerability state. The *Patch Published* date indicates when a vendor published a patch for a vulnerability, while the *Vulnerability Published* date indicates when the vulnerability was first published (for example, the date the CVE was published to NVD). The widget uses a heat map approach, with the upper left corner containing the vulnerabilities and patches that have been published in the last 30 days. Moving lower and to the right in the matrix, the colors change from yellow to



red as the risk levels increase. Tenable recommends remediating vulnerabilities shown in the lower right cells and working towards the upper left cells, since the lower right cells represent missing patches associated with vulnerabilities that have been known to the public for a longer period of time. Vulnerabilities displayed in this table are based on the plugins in the Local Security Checks plugin families for each Operating System, which will only run in an authenticated scan. Tenable provides a comprehensive collection of plugins for a large variety of operating systems to check for security issues, which are enumerated on the Tenable Plugins Page.	

Prioritize Using Prediction

Not everything can or should be patched. Take advantage of real-time threat intelligence to understand the latest attack paths used by ransomware groups to guide the organization's remediation strategy. Vulnerabilities targeted by ransomware exploits tend to cluster around specific types of weaknesses and asset categories. Savvy defenders can predict which vulnerabilities will likely be exploited in ransomware attacks and proactively address the risk before there is a business impacting event.

Predicting Likelihood of Vulnerability Exploitation

A Vulnerability Priority Rating (VPR) is expressed as a number from **0.1** to **10**, with higher values corresponding to a higher likelihood of the vulnerability leading to a compromise of the asset. Based on these values, vulnerabilities can be rated in terms of impact to the asset, including **Low (0.1-3.9)**, **Medium (4.0-6.9)**, **High (7.0-8.9)**, and **Critical (9.0-10.0)**.

> Note: The VPR is a machine-generated score based on the vulnerability alone, without regard to the environment where the vulnerability is found. Therefore, the VPR is not subject to user-specific considerations and cannot be changed or customized.

VPR is the output of the Predictive Prioritization process and is continually updated to accommodate the evolving threat landscape. Following the initial scan of an asset on the network, Tenable computes an initial VPR using a machine-learning algorithm that analyzes more than 150 different aspects of each vulnerability to determine the level of risk. The value is calculated within 24 hours of a vulnerability's initial disclosure in the National Vulnerability Database (NVD), providing security teams with early indicators of risk often days, weeks, and sometimes months before a CVSS value is assigned.

VPR is designed specifically for threat prioritization, unlike CVSS, which was designed to provide a static measure of technical severity. Relying on CVSS alone to prioritize vulnerabilities slows the assimilation of emerging threats, giving potential attackers an advantageous head start.

Key drivers that are used to calculate VPR include, but are not limited to, the following:

Key Driver	Description
Vulnerability	The number of days since the NVD published the vulnerability.

Key Driver	Description
Age	
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable.io displays a Tenable-predicted score using the text from the security advisory as an input.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of an exploit in various databases and frameworks, such as ReversingLabs, Exploit DB, Metasploit, Canvas, and more. The possible values (**High, Functional, PoC,** or **Unproven**) parallel the CVSS Exploit Code Maturity categories.
Product Coverage	The relative number of unique products affected by the vulnerability in the wild or in the current environment: **Low, Medium, High,** or **Very High**.
Threat Sources	A list of all sources, such as social media channels and the dark web, where threat events related to this vulnerability have occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: **Very Low, Low, Medium, High,** or **Very High**.
Threat Recency	The number of days **(0-730)** since a threat event occurred for the vulnerability.

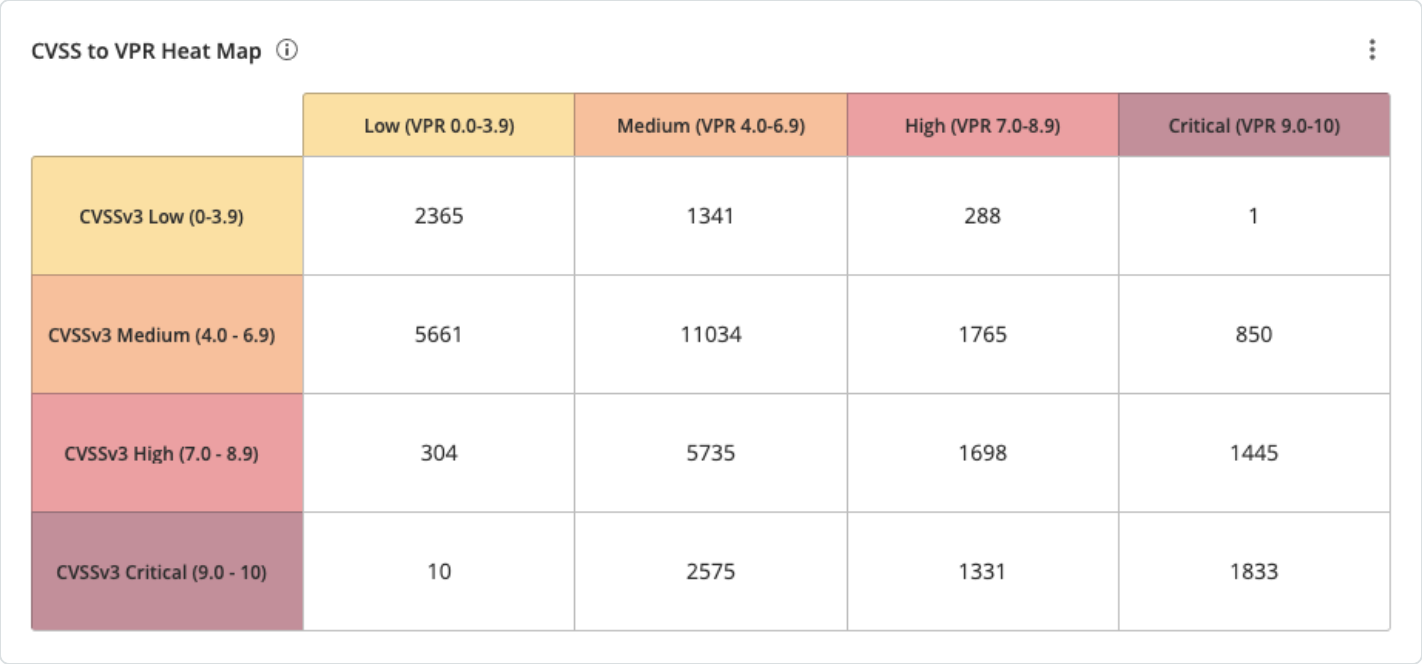
VPR integrates a broad range of dynamic risk factors to elevate the few vulnerabilities that require immediate attention, based on the level of risk for each vulnerability. Vulnerability overload has long been a pitfall of CVSS-based prioritization, which rates more than half of the vulnerabilities as “High” or “Critical." VPR, by comparison, rates very few vulnerabilities as “High” or “Critical," providing a more actionable basis for remediation planning. In fact, VPR is 18 times more efficient than CVSS in spotting vulnerabilities that are exploited by attackers. Tenable recommends resolving vulnerabilities with the highest VPR score first.

VPR Severity	VPR Score

Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Note: Vulnerabilities without CVEs in the NVD, such as many vulnerabilities with the *Info* severity, do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

The *CVSS to VPR Heat Map* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, provides a correlation between CVSSv3 scores and VPR scores for the vulnerabilities present in the organization. Each cell consists of a cross-mapping of CVSS & VPR scores. The widget uses a heat map approach, with the upper left corner containing the vulnerabilities with the lowest risk. Moving lower and to the right in the matrix, the colors change from yellow to red as the risk levels increase. Tenable recommends mitigating risks shown in the lower right cells and working towards the upper left cells, since the lower right cells represent the highest risk.



	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	2365	1341	288	1
CVSSv3 Medium (4.0 - 6.9)	5661	11034	1765	850
CVSSv3 High (7.0 - 8.9)	304	5735	1698	1445
CVSSv3 Critical (9.0 - 10)	10	2575	1331	1833

VPR is a key filter to prioritize the areas of the most significant concerns. Effective vulnerability remediation becomes easier as vulnerabilities that will cause the most significant impact float to the

top. VPR ratings can change over time, as threat intelligence information changes, which enables teams to focus on what is important right now. CVSS Vector filters are also used to prioritize returned results. Specific CVSS base metric options capture the characteristics of how a vulnerability is accessed and additional conditions that must exist to exploit the vulnerability. The following CVSS Vectors are used:

- **Access Complexity (AC) of Low (L)** means that the attack can be performed manually and requires little skill or information gathering to accomplish.
- **Access Vector (AV) of Network (N)** means that a vulnerability exploitable with Network Access is bound to the network stack and the attacker does not require local network or local access. This type of attack is commonly referred to as "remotely exploitable."
- **Authentication (Au) of None (N)** means Authentication is not required to exploit the vulnerability.

Combined with additional filters which focus on severity ratings and whether a vulnerability is exploitable or not, organizations become better equipped to see, predict, and take action to reduce risk across their entire attack surface. In addition to the above filters, the Vulnerability Published filter is used to filter vulnerability information related to vulnerabilities that have been identified as published in the last 30 days.

The *Exploitability By Attack Vector* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays exploitable vulnerabilities by the CVSS Exploitability Metric Vectors: **AV:N (Network), AV:A (Adjacent Network),** and **AV:L (Local)**. There is a row for each exploit framework. The CVSS metric vector specifies if the vulnerability is locally or remotely exploitable. The description for “Attack Vector” can be found in the First.org CVSS Specification Document.

Exploitability By Attack Vector

	Local	Network	Adjacent Network
Exploitable	2377	6016	170
Metasploit	589	955	45
Core	123	234	5
Canvas	169	439	1
Malware	1103	2744	17

Vulnerabilities that can be exploited remotely are a greater risk, since there is a global threat vector. Vulnerabilities that can be exploited locally require local access to the system through another mechanism, such as actions by an authorized user or access through a remote-execution vulnerability. Threat vectors are designated as Network (AV:N), Adjacent (AV:A), and Local (AV:L), as described below:

- **Network (AV:N)** Vulnerabilities that can be exploited with Network access are those where the vulnerable component is bound to the network stack and the attacker's path is through OSI layer 3 (the network layer). Such vulnerabilities are termed "remotely exploitable" and can exploited from one or more network hops away (i.e., across layer 3 boundaries from routers). An example of a network attack is an attacker causing a denial of service (DoS) by sending a specially crafted TCP packet from the public Internet. See also CVE-2004-0230.
- **Adjacent (AV:A)** Vulnerabilities that can be exploited with Adjacent network access are those where the vulnerable component is bound to the network stack. However, the attack is limited to the same shared physical network (such as Bluetooth, IEEE 802.11) or logical network (such as local IP subnet) and cannot be performed across an OSI layer 3 boundary, such as a router. An example of an Adjacent attack is an ARP (IPv4) or neighbor discovery (IPv6) flood leading to a denial of service on the local LAN segment. See also CVE-2013-6014.
- **Local (AV:L)** Vulnerabilities that can be exploited with Local network access are those where the vulnerable component is not bound to the network stack and the attacker’s path is through

read/write/execute capabilities. The attacker may be logged in locally to exploit the vulnerability or trick a user into executing malware.

Scan Web Applications

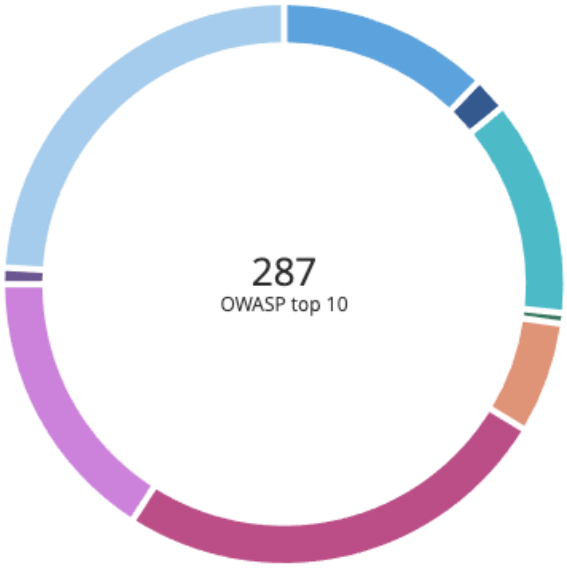
Organizations face several challenges when scanning web applications. The most common challenges include the identification of web application vulnerabilities among the aggregation of assets, scans returning an overwhelming number of vulnerabilities, and the scarcity of application security specialists.

Tenable.io Web App Scanning (WAS) provides easy-to-use, comprehensive, and automated vulnerability scanning for modern web applications, enabling security and development teams to quickly configure and manage web app scans in a matter of minutes with minimal tuning. For more information, read the Tenable.io white paper and guide, Getting Started with Web Application Scanning.

Whether purchased as a module of Tenable.io Vulnerability Management or as a core component of the Tenable Exposure Platform (Tenable.ep), Tenable.io WAS provides this visibility as part of a comprehensive Cyber Exposure solution. Tenable.io WAS provides high detection rates with minimal false positives, revealing the true cyber risk in web applications. This enables security teams to view identified vulnerabilities to ensure visibility and prioritize remediation.

The *Top 2017 OWASP Categories Discovered in the Last 14 days* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays the percentages of active Web Application vulnerabilities from Tenable.io WAS by OWASP category.

Top 2017 OWASP Categories Discovered (Last 14 Days)



- 12% A1 - Injection
- 2% A2 - Broken Authentication
- 13% A3 - Sensitive Data Exposure
- <1% A4 - XML External Entities (XXE)
- 6% A5 - Broken Access Control
- 26% A6 - Security Misconfiguration
- 16% A7 - Cross-Site Scripting (XSS)
- 1% A8 - Insecure Deserialization
- 24% A9 - Using Components with Known Vulnerabilities

Avoid Scanning Fragile Devices

There are many fragile devices on each network that cannot be included in active scanning, due to the sensitive nature of such devices. Operational Technology (OT) is the most common category of sensitive devices. OT refers to programmable systems or devices that interact with a physical environment, such as Internet of Things (IoT) devices, and Industrial Control Systems (ICS). The common practice within OT environments is to avoid using active scanning approaches because of the risk of degradation or disruption of service. Due to IT/OT Convergence, IT and OT networks are no longer as segregated as they were in the past, so it is common to find OT devices on the IT network and vice versa. This raises the importance placed on an organization's scanning strategy.

Tenable uses ICS/SCADA Smart Scanning by default to safely identify OT devices and stop scanning them once they are discovered. ICS/SCADA Smart Scanning reduces the number of plugins run against fragile devices by 90%. This eliminates the plugins that put the greatest load on the device, including HTTP and SSH testing. On the scan configuration page, under Settings > Discovery > Fragile Devices, the *Scan Operational Technology devices* slider is disabled by default, which turns on ICS/SCADA Smart Scanning. If the slider for *Scan Operational Technology devices* is enabled, the scanner **will** perform a full scan of OT devices, such as programmable logic controllers (PLCs) and Remote Terminal Units (RTUs) that monitor environmental factors and the activity and state of machinery. Tenable does **not** recommend enabling this setting, whether scanning an "IT" or an "OT" network.

Tenable.ot can be used to safely and comprehensively gain visibility into an OT environment. Tenable.ot uses passive monitoring and communication in each device's proprietary protocol since these methods do not interfere with OT devices. A restricted version of the Nessus scanner is included in Tenable.ot to permit scanning of the non-sensitive OT devices, such as Human Machine Interfaces (HMIs), Historians, and network devices. Tenable.io and Tenable.ot work together to provide a unified view of IT and OT security. Check out the Getting Started with Tenable.ot Dashboard for Tenable.io.

Continue reading for more information about *ICS/SCADA Smart Scanning*, which can be used to identify devices to add to the "do not scan" list.

ICS/SCADA Smart Scanning identifies OT devices and stops scanning them once discovered. The following list provides further details of *ICS/SCADA Smart Scanning*:

1. Smart Scanning pings the IP address to determine if a device is using that address.
2. Smart Scanning probes against open known OT ports and protocols. Initially supported protocols include Siemens S7, Modbus, BACnet, Omron FINS, Ethernet CIP, 7T IGSS, and ICCP COTP.
3. When an OT port or protocol is identified, Nessus will report the open ports and protocol found. Many of the protocols include INFO or QUERY commands to capture basic information about the device, such as the device type. Nessus records the information provided by the device protocol.
4. The scan stops for that device. Plugin 109142 results show the OT device when an OT protocol was identified and normal scans of OT devices were not enabled.
5. The devices listed by plugin 109142 can be added to the “do not scan” list.

Using Tenable.ad to Identify Active Directory Exposures

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. For information about how to identify AD exposures, see the Tenable blog, How to Protect Active Directory Against Ransomware Attacks.

Reduce Privileged AD Group Membership

Microsoft recommends reducing the use of privileged accounts in an AD domain to the bare minimum. Limit membership to groups such as *Domain Admins*, *Enterprise Admins*, and *Schema Admins* to only staff who require privileged access, and review these groups on a regular basis.

Example: Enumerate Users and Groups

Plugin 69239 - Active Directory, Enumerate Users and Groups

Queries Active Directory for a list of Users and their Group Memberships by retrieving a list of Users and Groups via ADSI.

> **Tip**: Audit the membership of privileged AD groups to limit membership levels.

Restrict the Use of Privileged AD Accounts

There are some technologies in Windows that can help reduce the exposure of privileged AD credentials, such as the *Protected Users* and *Windows Defender Credential Guard* groups. Follow Microsoft's recommendations and limit the use of privileged AD accounts to devices that are secured for the purpose of administering AD.

Example: Account Operators Group

Plugin: 10901 - Microsoft Windows 'Account Operators' Group User List

Members of this group can create or modify local user accounts but cannot modify or create administrative accounts or edit user rights.

Tip: Create a set of Privileged Access Workstations (PAW) used exclusively for performing administrative tasks that require privileged access to AD.

Manage End-User Devices Using a Local Account

Organizations generally grant remote access to clients using a domain user account. Microsoft's *Local Administrator Password Solution (LAPS)* tool provides a more secure method for remote support by randomizing and periodically changing the local administrator password on devices. Using a local account to support end user devices makes it difficult for attackers to compromise AD.

Example: Windows Local Administrators Group

10902 - Microsoft Windows 'Administrators' Group User List

Members of this group have complete access to the system.

Tip: Audit local administrator account passwords to make sure that each device has a unique local administrator account password. Do not use domain accounts for remote support.

Protect Privileged AD Accounts with Multi-Factor Authentication

Many organizations rely on passwords alone to protect privileged AD accounts. According to Microsoft, Multi-Factor Authentication (MFA) is proven to block 99.9% of automated attacks. MFA requires users to provide something in addition to their password, such as a biometric gesture or one-time passcode generated by an authenticator app.

Tip: Add MFA to Windows Server Active Directory. Azure MFA and other products can be used to add MFA to AD.

Following Microsoft's security advice is a good starting point to secure AD and to stop attackers from using AD to spread ransomware. However, the server management tools built into Windows Server do not provide a way to monitor AD in real time, nor do they supply the threat intelligence needed to automate responses in an evolving threat landscape. Tenable.ad can identify security issues within AD before attackers exploit the flaws and spread ransomware. The built-in knowledge and threat intelligence helps organizations mitigate issues and remediate threats. Tenable.ad integrates with SIEMs and other security tools to proactively improve AD security, providing dynamic dashboards to provide insights that would not exist without specialized security software.

Monitor AD for Unusual Activity

Just as anti-malware software scans Windows for unusual files and processes, AD must be monitored for unusual activity. The Windows Event Log contains a great deal of information that could reveal misuse of privileged accounts and other malicious behavior. With the right data, organizations can proactively stop the spread of ransomware attacks via AD. SIEM products can be used to collect information forwarded from the Windows Server Event Log and other systems. Threat intelligence can provide an automated way for organizations to identify threats in the data collected from security events. Neither Windows Logs nor SIEM products are sufficient when used on their own.

> **Tip**: Deploy a SIEM with threat intelligence to proactively block ransomware and other types of malware before infection of the entire network occurs.

Implement a Tiered Administration Model for AD

Microsoft recommends using a secure tiered model to organize AD resources. The model defines three tiers that serve as buffers to separate the administration of high-risk devices, such as end-user PCs and valuable servers, such as domain controllers. Tier 0 includes resources such as privileged AD accounts, domain controllers, and Privileged Access Workstations (PAWs). Tier 1 is used for member services and applications. Tier 2 is used for end-user PCs and the objects in AD that are used to manage PCs, such as help desk user accounts.

> **Tip**: Using a phased approach, reorganize AD so that a tiered administration model is used.

AD changes, syslog changes, and Windows event logs can be correlated with threat intelligence to reveal misuse of privileged accounts and active misconfiguration exploits. This technology enables incident response teams to proactively prevent ransomware attacks from spreading via AD. Integrate this data with a SIEM to collect information forwarded from the Windows Server event logs and other systems.

AD Plugins, Scan Templates, Widgets, and Dashboards

The *Active Directory Starter Scan Template* contains 10 hygiene checks that are often exploited by attackers to navigate target ADs. These plugins focus on the two most common attack paths to help prevent attackers from guessing or cracking accounts, impersonating other users, and limits the ability for attackers to escalate privileges and move across domains. Specifically, these checks help

organizations to identify attacks that are difficult to detect, such as Golden Ticket attacks. Along with legacy protocols, weak passwords, and accounts with elevated privileges, Golden Ticket Attacks are the most common attack against AD servers. Golden Ticket attacks, such as Kerberoasting, center around Kerberos and KRBTGT (Kerberos Ticket Granting Ticket), which are typically launched from inside the network. Kerberoasting is an attack that enables privilege exploitation, furthering the ability of an attacker to move laterally in the network.

These attacks are dangerous because the attacker does not require administrative rights. An attacker can simply request a service ticket from the Domain Controller and use password cracking tools offline to retrieve plain text credentials from vulnerable hashes. AD vulnerabilities that can be a benefit to attackers are also identified, such as Null Sessions, Primary Group ID, Weak Encryption, and Dangerous Trust Relationships.

The following plugins are part of the *Active Directory Starter Scan Template* and are intended to be used for preliminary analysis of AD hosts.

- 150480 **AD Starter Scan – Kerberoasting** A privileged account is vulnerable to the Kerberoasting attack.
- 150481 **AD Starter Scan – Weak Kerberos Encryption** A weak Kerberos algorithm is configured on a user account.
- 150482 **AD Starter Scan – Kerberos Pre-Authentication Validation** Kerberos pre-authentication is disabled on a user account.
- 150483 - **AD Starter Scan - Non-Expiring Account Password** Accounts with never expiring passwords.
- 150484 - **AD Starter Scan - Kerberos Krbtgt** KDC last password change is too old.
- 150485 **AD Starter Scan – Unconstrained Delegation** Dangerous Kerberos delegation is set.
- 150486 **AD Starter Scan - Dangerous Trust Relationship** A dangerous configuration on an outbound trust relationship is configured.
- 150487 **AD Starter Scan - Primary Group Identity** A potential backdoor using the Primary Group ID attribute has been found on a user account.
- 150488 **AD Starter Scan – Null Sessions** The Anonymous or Everyone foreign security prin-

cipal is part of the Pre-Windows 2000 Compatible Access group.

- 150489 **AD Starter Scan - Blank Passwords** An account may have an empty password.

For more information about the issues discovered by the *Active Directory Starter Scan* plugins, please refer to the Tenable Blog, Find and Fix These 10 Active Directory Misconfigurations.

In addition to the AD plugins and scan template, the Getting Started with Active Directory Tenable.io Dashboard, is available to quickly discover and analyze basic AD weaknesses. The AD plugins and scan template are available in Nessus Essentials, Nessus Professional, Tenable.sc, Tenable.io, and Tenable.ep.

The *Microsoft Active Directory Findings* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays Active Directory vulnerabilities using the CPE filter for *cpe:/a:microsoft:active_directory*.

Microsoft Active Directory Findings

PLUGIN ID	NAME	SEVERITY	VULN TOTAL
150489	AD Starter Scan - Blank passwords	Medium	2
150484	AD Starter Scan - Kerberos Krbtgt	Medium	2
150483	AD Starter Scan - Non-Expiring Account Password	Medium	2
150480	AD Starter Scan - Kerberoasting	High	2
69556	Active Directory - Enumerate User Account Policy	Info	2
69239	Active Directory - Enumerate Users and Groups	Info	2
69238	Active Directory - Enumerate Group Memberships	Info	2
69236	Active Directory - Enumerate Computer Objects	Info	2

Mitigation

Verify Mitigation

Frequently, vulnerabilities targeted for remediation are never fully remediated. While security teams are responsible for detecting and prioritizing vulnerabilities, patching the vulnerabilities is the responsibility of IT staff and developers who speak a different language and have different goals. Integration of Risk-Based Vulnerability Management (RBVM) solutions with ITSM and ticketing systems is of the utmost importance to automate workflows, correlate vulnerabilities with patches, and verify that all instances of a vulnerability have been patched or remediated by a compensating control. Use authenticated scans to ensure that patches are activated, not just installed, since some patches require a system reboot or a registry change.

Track Progress

Tenable assigns a vulnerability state to all vulnerabilities detected on the network: **New, Active, Fixed,** and **Resurfaced**. The Vulnerability state *Fixed* is assigned when the vulnerability was present on a host, but is no longer present. This vulnerability state can be used to track vulnerabilities that were previously *New* or *Active* and have now been remediated. Vulnerabilities that have been marked as *Fixed* are no longer displayed in the active vulnerability dashboards and workbenches but can be found when using the *Vulnerability State* filter for *Fixed*. If a vulnerability was previously marked as *Fixed* and returns to the host, that vulnerability will be marked as *Resurfaced* and will re-appear in the active vulnerability dashboards and workbenches.

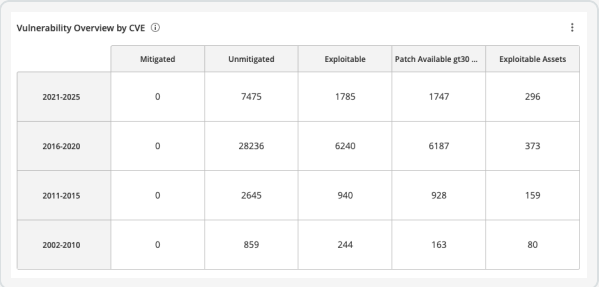
Measure Performance

Successful teams take time to reflect on their performance, and security is no different. This requires developing key metrics to measure and communicate how operational controls are working (or not working) and benchmarking data to compare performance across internal groups or externally against peers. Generate metrics that cover foundational cyber hygiene practices, such as assessment capabilities, remediation speed, and overall risk reduction.

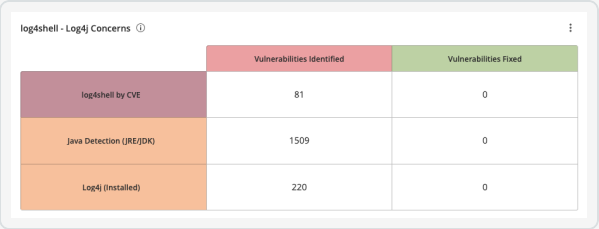
Widget Description	Widget Image

The *Vulnerability Overview by CVE* Widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays a count of the following:

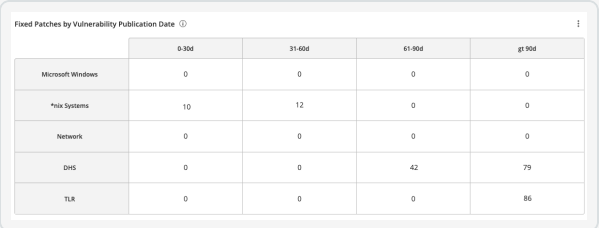
- Mitigated (**Fixed**) Vulnerabilities
- Unmitigated (**New, Active,** or **Resurfaced**) vulnerabilities
- Exploitable vulnerabilities
- Vulnerabilities with a patch available
- Vulnerabilities with an exploit available



The **Fixed** *Vulnerability State* filter displays vulnerability findings that have been fixed and can be combined with other filters, such as the CVE filter, in workbench searches and custom widgets. While Tenable provides dashboard templates, such the Defending Against Ransomware (ACT) Tenable.io Dashboard, users have the ability to create custom widgets for their specific requirements. The *log4shell - Log4j Concerns* pre-configured widget uses the **Fixed** *Vulnerability State* filter with the CVE filter to display fixed Log4j and Java vulnerabilities.



The *Fixed Patches by Vulnerability Publication Date* widget, which can be found in the Defending Against Ransomware (ACT) Tenable.io Dashboard and Tenable.io widget library, displays counts of fixed vulnerabilities grouped by the patch publication



date. This matrix assists organizations with mapping mitigation progress and presents data to determine whether organizational SLAs are being met. Each cell contains a count of fixed vulnerabilities grouped by Microsoft Windows systems, *nix systems, Network devices, and vulnerabilities specified in the DHS BOD 22-01 and Tenable's 2021 Threat Landscape Retrospective with a patches published 0-30, 31-60, 61-90, and more than 90 days ago.	

Learn More

Tenable Resources

- Defending Against Ransomware (ACT) Tenable.io Dashboard
- Tenable Plugins Page
- Tenable's coverage of Log4j
- Tenable's coverage of Apache Struts
- CVE-2021-30116: Multiple Zero-Day Vulnerabilities in Kaseya VSA Exploited to Distribute REvil Ransomware
- Get the E-book: Anatomy of a Modern Ransomware Attack
- Read the blog: How to Measure the Efficacy of Your Cybersecurity Program: 5 Questions to Ask
- View the webinar: Introducing Tenable.ad – Secure Active Directory and Disrupt Attack Paths
- Download the E-Book: A King's Ransom: How to Stop Ransomware Spreading via AD
- Download the Tenable.io Web Application Scanning (WAS) Guide

External Resources

- National Institute of Standards (NIST) Special Publication 800-53
- Payment Card Industry Data Security Standard (PCI DSS)
- NIST Mapping to HIPAA Security Rule
- General Data Protection Regulation (GDPR)
- Center for Internet Security (CIS)
- ISO 27002: 2013 Security Standards
- CISA Known Exploited Vulnerabilities Catalog
- OWASP Top Ten