COMPANY NAME

WatchGuard Endpoint Risk Assessment

1 May 2023 – 19 June 2023

Duration: 25 days

Number of Endpoints: 34

CYBERSECURITY

Contents

CYBERSECURITY

1. Summary

Security risks discovered in the assessment.

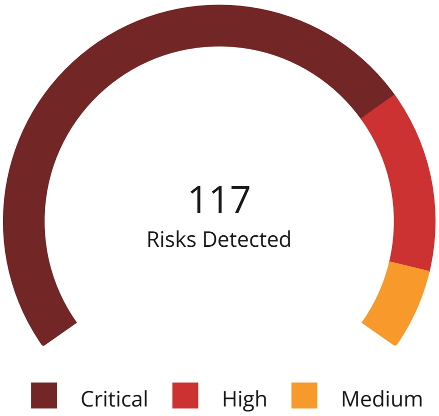
SUMMARY

1.1 Risk Summary

This section shows the total number of security risks discovered in the assessment based on their type and severity:

- **Critical:** Indicates confirmed malicious payloads were executed or there was a dangerous level of exposure to a cyberattack.
- **High:** Points to latent malware that could be executed at any time or an urgent need to reduce the attack surface.
- **Medium:** Designates additional risk factors that should be addressed preventively.

Overall Company Risk



84
Critical Risks

14	Active malware
9	Active potentially unwanted programs
8	Exploits executed
35	Network attacks detected
18	Indicators of Attack (Critical risk)
0	Known actively exploited vulnerabilities

23
High Risks

9	Malware detected by scans
2	Potentially unwanted programs detected by scans
9	Indicators of Attack (High risk)
3	Other critical security vulnerabilities

10
Medium Risks

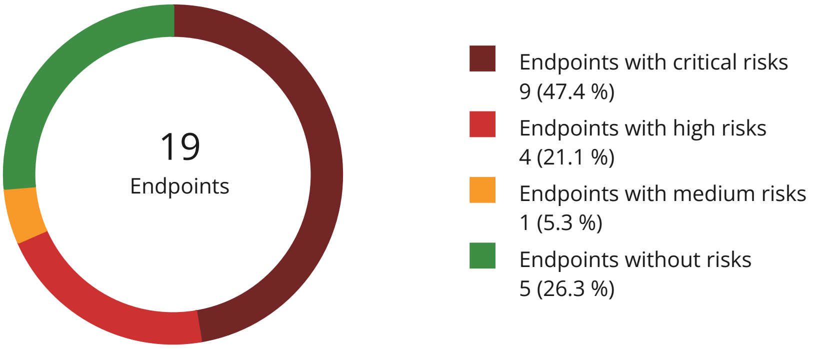
0	Applications with high download data volume
0	Applications with high upload data volume
0	LOTL applications executed
3	EOL software installed
4	Indicators of Attack (Medium risk)
3	Important security vulnerabilities

SUMMARY

1.2 Endpoint Risk Status

Endpoints identified with risks can mean that there is no protection installed. It could also mean that the protection installed is not properly configured or updated.

Endpoints with Risks



High-Risk Endpoints

These are the endpoints with the highest risk.

1. WIN-DESKTOP-1 (192.168.0.205)

4	Active malware	**1**	Active potentially unwanted programs
3	Exploits executed	**7**	Network attacks detected
4	Indicators of Attack (Critical risk)		
1	Indicators of Attack (High risk)	**1**	Malware detected by scans

2. WIN-DESKTOP-3 (192.168.0.5)

5	Active malware	**7**	Network attacks detected
6	Indicators of Attack (Critical risk)		
1	Indicators of Attack (High risk)		
2	Indicators of Attack (Medium risk)		

3. WIN-SERVER-2 (192.168.0.108)

5	Active potentially unwanted programs
2	Indicators of Attack (Critical risk)
4	Indicators of Attack (High risk)
1	Indicators of Attack (Medium risk)
7	Network attacks detected

4. WIN-DESKTOP-2 (192.168.0.123)

1	Active malware
1	Exploits executed
1	Malware detected by scans
1	Active potentially unwanted programs
7	Network attacks detected

5. WIN-SERVER-1 (10.17.69.1)

1	Active malware
7	Network attacks detected
1	Indicators of Attack (High risk)
1	Exploits executed

SUMMARY

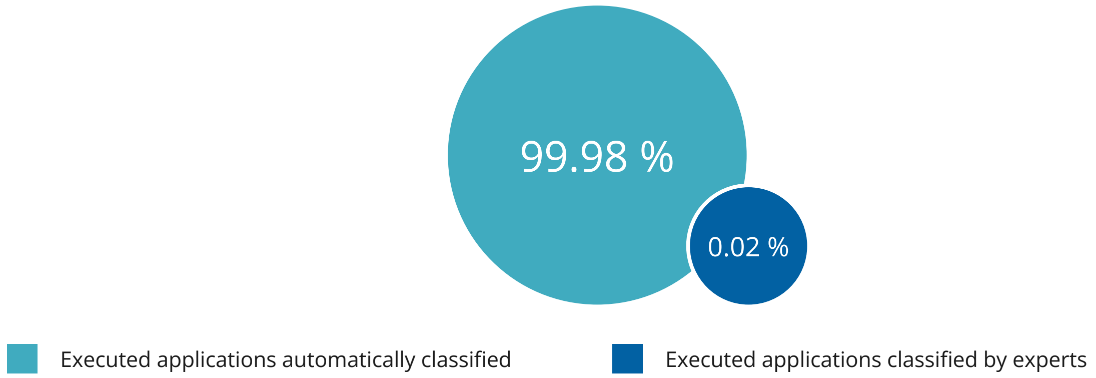
1.3 Zero-Trust Application Service Assessment

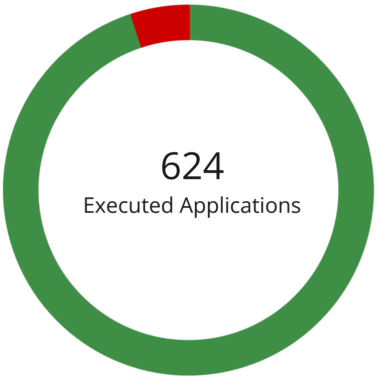
The Zero-Trust Application Service is a managed service included as part of the WatchGuard Endpoint Security solution. It classifies application binary files as either Trusted or Malware, and can be configured to only allow trusted applications to run on managed endpoints.

30,000M+	8 trillion+	5M+
Events per day	Events in the data lake	New binaries classified per week

In the context of this assessment, the service might have identified several unknown application files that were deemed trustworthy or determined to be zero-day malware. While this process is mostly AI-based, a team of WatchGuard experts reviews an average of 0.02% of all the files not automatically processed.

For more information about the Zero-Trust Application Service, you can review this **Feature Brief.**





Zero-Trust Application Service assessment output

🟩 Applications classified as trusted – 593 (95.0 %)

🟥 Applications classified as malware or PUP[1] – 31 (5.0 %)

[1] Of the total number of applications classified as malware or PUP, **0 %** were classified as zero-day malware.

Endpoints with Unknown Applications

0 % of the endpoints have executed Unknown Applications.

SUMMARY

1.4 Threat Hunting Service Assessment

WatchGuard's continuous real-time monitoring of endpoint activity enables the WatchGuard Endpoint Agent to act as a sensor and inform the cloud platform about files being run and their execution context. For example, we can determine what happened before and after execution, the specific commands issued by users or parameters included, the types of network traffic generated, and the data files that were accessed.

This enables our Threat Hunting Service to focus on living-off-the-land (LotL), fileless and malwareless attacks. The Threat Hunting Service can identify abnormal behaviors as well as suspicious activity, ultimately generating high-fidelity IOAs (Indicators of Attack) when it confirms the early stages of an attack.

For more information about the Threat Hunting Service, you can review this **Feature Brief.**

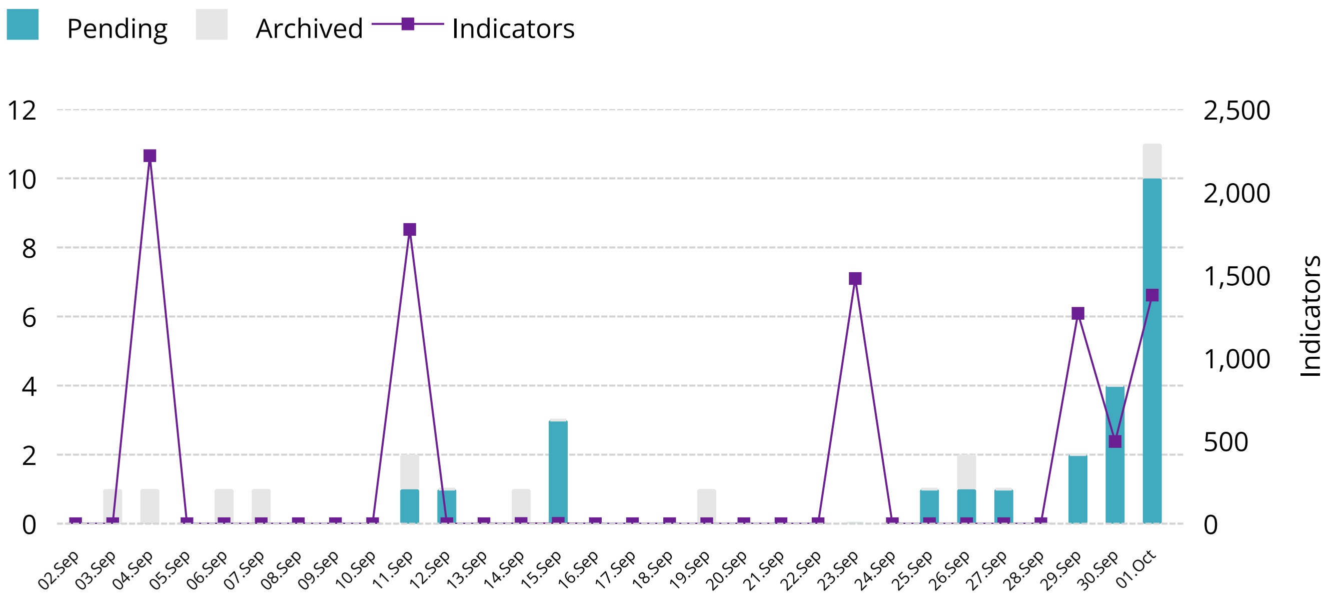
Threat Hunting Service Assessment Output

88,769
Events

8,621
Indicators

33
Indicators of Attack (IOAs)

Detection Trends



Events

Events are any relevant action that is monitored by WatchGuard Endpoint Security. The processes and applications that run on endpoints generate a stream of events that are sent to the cloud, where they are stored so that analysts can later investigate each event individually or in relation to others. Rest assured that personally identifiable information is never included in event details.

Indicators

An indicator is triggered when a **hypothesis** created by the WatchGuard Threat Hunting team matches the events received from the WatchGuard Endpoint Agent.

Indicators of Attack (IOAs)

IOAs are reviewed and confirmed indicators with a high probability of corresponding to an attack. These attacks are typically at an early or exploitation stage and often do not use file-based malware.

CYBERSECURITY

2. Assessment Details and Recommendations

Review detailed information and recommendations for every risk type we detected — malware, PUPs, exploits, IOAs, and more.

DETAILS AND RECOMMENDATIONS

2.1 Malware Detected

This table provides information about the various forms of malicious software discovered during the assessment, including ransomware, trojans, worms, spyware, viruses, and even targeted attack components. These might have been detected by the endpoint sensor in real-time at the point of entry, when actively taking actions in compromised endpoints, or they simply were present in the file system.

Each detection reports whether the malware was executed at some point, if it accessed data files (including hundreds of different formats, from text documents to databases), or if it established network connections.

Latest Active Malware Detections

Endpoint	Threat	⚡	🗎	🌐	Date
WIN-SERVER-1	Trj/Chgt.J	○	○	○	10/1/2023 11:05 PM
WIN-DESKTOP-3	W32/Exploit.gen	○	○	○	10/1/2023 5:43 PM
WIN-DESKTOP-3	W32/Exploit.gen	○	○	○	10/1/2023 5:40 PM
WIN-DESKTOP-1	PUP/AskToolbar	●	○	●	10/1/2023 12:30 PM
WIN-DESKTOP-1	Trj/iexplore.exe	○	○	○	10/1/2023 12:20 PM
WIN-DESKTOP-1	Trj/Teams.exe	○	○	○	10/1/2023 12:20 PM
WIN-DESKTOP-3	W32/Exploit.gen	○	○	○	10/1/2023 8:51 AM
WIN-SERVER-1	Trj/Genetic.gen	●	○	●	10/1/2023 8:16 AM
WIN-SERVER-1	Trj/RansomCrypt.C	●	○	○	10/1/2023 7:13 AM
WIN-DESKTOP-1	Trj/CryptoWall.A	○	○	○	10/1/2023 5:25 AM

⚡ Executed 🗎 Accessed data files 🌐 Established network connections

Latest Malware Detected By Scans

Endpoint	IP	Group	Detections	Date
WIN-DESKTOP-2	192.168.0.123	Workstation	1	10/1/2023 11:46 PM
LINUX-DESKTOP-1	192.168.0.116	Root	1	10/1/2023 11:45 PM
LINUX-LAPTOP-1	192.168.0.35	Root	1	10/1/2023 11:45 PM
WIN-DESKTOP-5	192.168.0.140	Workstation	1	10/1/2023 11:44 PM
WIN-DESKTOP-1	192.168.0.205	Workstation	1	10/1/2023 11:43 PM
WIN-DESKTOP-5	192.168.0.140	Workstation	1	9/27/2023 6:41 PM
WIN-DESKTOP-5	192.168.0.140	Workstation	1	9/15/2023 3:31 AM
WIN-DESKTOP-5	192.168.0.140	Workstation	1	9/6/2023 5:25 PM
MAC-DESKTOP-2	192.168.0.198	Root	1	9/3/2023 6:05 PM

Recommendations

Discovering malware in corporate systems can be concerning. In the case of active malware, you should take immediate action. You might also want to obtain expert security guidance to both assess the nature of the threat and eradicate the malware.

- Isolate the affected endpoints from the network to prevent further impact on other endpoints.
- Remove all malware from the endpoints where it was detected as soon as possible to increase baseline security and to prevent lateral movement to other endpoints.
- Deploy an advanced endpoint security solution on all endpoints to avoid future compromise.
- Make sure your endpoint security solution is up to date and configured according to best practices.

DETAILS AND RECOMMENDATIONS

2.2 Potentially Unwanted Programs (PUPs) Detected

This table lists threats classified as PUPs, such as spyware, hacking tools, and toolbars, that were discovered during the assessment. The WatchGuard Endpoint Agent might have detected them in real time at the point of entry, when they executed, or they might have already been present in the file system.

PUPs are typically installed on an endpoint or device without the explicit consent or even awareness of the user. They often cause inconveniences, security risks, and undesirable behavior. They can increase network traffic, degrade overall system performance, or cause incompatibilities with installed software.

Latest Active PUP Detections

Endpoint	Threat	⚡	📄	🌐	Date
WIN-SERVER-1	HackingTool/VulnerabilityScanner	●	○	○	10/1/2023 7:01 AM
WIN-SERVER-2	Trj/PUP.EXE	●	●	○	10/1/2023 5:15 AM
WIN-SERVER-2	Trj/BLToPUP1.exe	●	●	○	10/1/2023 5:15 AM
WIN-SERVER-2	Trj/BLToPUP2.exe	●	●	○	10/1/2023 5:15 AM
WIN-SERVER-2	Trj/WLT.N	●	●	●	10/1/2023 4:24 AM
WIN-SERVER-1	Trj/WLT.C	●	●	●	10/1/2023 4:23 AM
WIN-DESKTOP-2	Trj/WLT.C	●	●	●	10/1/2023 4:15 AM
WIN-DESKTOP-1	Trj/WLT.D	●	●	●	10/1/2023 4:15 AM
WIN-SERVER-2	PUP/SoftwareUpdater	●	○	●	10/1/2023 4:13 AM

⚡ Executed 📄 Accessed data files 🌐 Established network connections

Latest PUP Detected By Scans

Endpoint	IP	Group	Detections	Date
MAC-DESKTOP-2	192.168.0.198	Root	1	10/1/2023 11:45 PM
WIN-DESKTOP-5	192.168.0.140	Workstation	1	9/23/2023 1:38 PM

Recommendations

Not all PUPs are harmful or malicious. Some legitimate software may be categorized as a PUP due to behavior or certain undesirable characteristics. PUPs should be regularly reviewed and removed from systems to increase baseline security and endpoint integrity.

- Make sure an endpoint security solution is deployed on all endpoints to avoid future occurrences.

- If you already have an endpoint security solution deployed, make sure it is up to date and configured according to best practices.

DETAILS AND RECOMMENDATIONS

2.3 Exploits Detected

Anti-exploit technology is an important endpoint protection layer that prevents lateral movement by mitigating existing software vulnerabilities before a vendor patch is released (virtual patching). WatchGuard’s anti-exploit technology includes detections based on the anomalous behavior of exploited processes. It is an important addition to any patch management strategy to harden systems against vulnerable applications, as well as environments still running end-of-life software or legacy operating systems.

This table lists programs and exploit techniques detected on your endpoints.

Latest Exploit Detections

<table>
<tr><th>Endpoint</th><th>Compromised Program</th><th>Exploit Technique</th><th>ϟ</th><th>Date</th></tr>
<tr><td>WIN-DESKTOP-1</td><td>3|DESKTOPDIRECTORY|\V2.4 User Cases\HitmanPro\Hitmanpro.exe</td><td>Exploit/HookBypass</td><td>●</td><td>10/1/2023 5:09 PM</td></tr>
<tr><td>WIN-DESKTOP-1</td><td>3|SYSTEM|\apc.exe</td><td>Exploit/APC_Exec</td><td>○</td><td>10/1/2023 3:22 PM</td></tr>
<tr><td>WIN-SERVER-1</td><td>WINDOWS|\bonjour.EXE</td><td>Exploit/Metasploit</td><td>○</td><td>10/1/2023 12:30 PM</td></tr>
<tr><td>WIN-DESKTOP-5</td><td>WINDOWS|\lsass.EXE</td><td>Exploit/DumpLsass</td><td>○</td><td>10/1/2023 12:30 PM</td></tr>
<tr><td>WIN-DESKTOP-5</td><td>A03|DESKTOPDIRECTORY|\testWSA\33\powershell.exe</td><td>Exploit/PsSuspiciousCommand</td><td>●</td><td>10/1/2023 11:36 AM</td></tr>
<tr><td>WIN-DESKTOP-5</td><td>A03|DESKTOPDIRECTORY|\testWSA\32\powershell.exe</td><td>Exploit/PsSuspiciousCommand</td><td>●</td><td>10/1/2023 11:36 AM</td></tr>
<tr><td>WIN-DESKTOP-2</td><td>3|SYSTEMDRIVE|\ExploitTester_Release\url\iexplore.exe</td><td>Exploit/IE_GodMode</td><td>○</td><td>10/1/2023 9:38 AM</td></tr>
<tr><td>WIN-DESKTOP-1</td><td>TEMP\7C62153392561255386e5f059c2161cd</td><td>Exploit/ROP1</td><td>●</td><td>10/1/2023 4:33 AM</td></tr>
</table>

ϟ Executed

Recommendations

It is important to patch vulnerabilities in detected compromised programs as soon as possible. It is critical to keep all operating systems and software up to date to mitigate the chances of exploitation.

- Stay up to date with announcements from vendors and other reliable sources and apply patches when they become available.
- Consider engaging security experts to assess potential impacts and implement additional remediation measures if necessary.
- Implement a robust endpoint security solution that employs behavior monitoring and anomaly detection mechanisms, helping you build a patch and vulnerability management program.

DETAILS AND RECOMMENDATIONS

2.4 Network Attacks Detected

Many cyberattacks start with exploiting vulnerabilities in Internet-exposed services. Network attacks take advantage of vulnerabilities, misconfigurations, or design flaws in network systems, and are typically carried out by attackers who attempt to leverage these weaknesses to compromise network security and gain unauthorized access. If there is already a level of network compromise, the attack could ultimately need to be stopped at the endpoint.

For example, these methods or exploits have been commonly used to target specific vulnerabilities:

- **EternalBlue**
  Exploits the CVE-2017-0144 vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol. Windows endpoints not patched against this vulnerability can allow illegitimate data packets with malware such as a trojan or ransomware.

- **BlueKeep**
  Exploits the CVE-2019-0708 vulnerability on Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Vista, and Windows XP endpoints. The threat has the potential to devastate networks as it can spread between endpoints as a worm.

- **Zerologon**
  Exploits the CVE-2020-1472 vulnerability in the cryptography of Microsoft\'s Netlogon process to allow an attack against Microsoft Active Directory domain controllers. Zerologon makes it possible for a hacker to impersonate any computer, including the root domain controller.

Latest Network Attack Detections

Endpoint	Network Attack	Local IP Address	Remote IP Address	Date
WIN-DESKTOP-2	Denial of Service attack (DoS)	192.168.2.11	172.100.25.22	10/1/2023 10:38 AM
WIN-DESKTOP-3	Denial of Service attack (DoS)	192.168.2.11	172.100.25.22	10/1/2023 10:38 AM
WIN-DESKTOP-1	Denial of Service attack (DoS)	192.168.2.11	172.100.25.22	10/1/2023 10:38 AM
WIN-SERVER-1	Denial of Service attack (DoS)	192.168.2.11	172.100.25.22	10/1/2023 10:38 AM
WIN-SERVER-2	Denial of Service attack (DoS)	192.168.2.11	172.100.25.22	10/1/2023 10:38 AM
WIN-SERVER-1	Cross-Site Scripting attack (XSS)	192.168.1.24	172.20.1.24	10/1/2023 8:35 AM
WIN-SERVER-2	Cross-Site Scripting attack (XSS)	192.168.1.24	172.20.1.24	10/1/2023 8:35 AM
WIN-DESKTOP-1	Cross-Site Scripting attack (XSS)	192.168.1.24	172.20.1.24	10/1/2023 8:35 AM
WIN-DESKTOP-3	Cross-Site Scripting attack (XSS)	192.168.1.24	172.20.1.24	10/1/2023 8:35 AM
WIN-DESKTOP-2	Cross-Site Scripting attack (XSS)	192.168.1.24	172.20.1.24	10/1/2023 8:35 AM
WIN-DESKTOP-2	Unauthorized access	192.168.1.1	172.100.10.2	10/1/2023 8:25 AM
WIN-DESKTOP-1	Unauthorized access	192.168.1.1	172.100.10.2	10/1/2023 8:25 AM
WIN-SERVER-2	Unauthorized access	192.168.1.1	172.100.10.2	10/1/2023 8:25 AM
WIN-DESKTOP-3	Unauthorized access	192.168.1.1	172.100.10.2	10/1/2023 8:25 AM
WIN-SERVER-1	Unauthorized access	192.168.1.1	172.100.10.2	10/1/2023 8:25 AM
WIN-SERVER-1	Man in the middle attack (MITM)	192.168.2.11	172.100.25.22	10/1/2023 7:38 AM
WIN-DESKTOP-1	Man in the middle attack (MITM)	192.168.2.11	172.100.25.22	10/1/2023 7:38 AM
WIN-SERVER-2	Man in the middle attack (MITM)	192.168.2.11	172.100.25.22	10/1/2023 7:38 AM
WIN-DESKTOP-3	Man in the middle attack (MITM)	192.168.2.11	172.100.25.22	10/1/2023 7:38 AM
WIN-DESKTOP-2	Man in the middle attack (MITM)	192.168.2.11	172.100.25.22	10/1/2023 7:38 AM

Recommendations

An endpoint-based network attack protection layer detects and stops threats by inspecting network traffic in real time to prevent service-centric attacks at an early stage.

- Make sure you disable any network services you do not need.
- Perform periodic vulnerability scans and assessments on network devices, systems, and applications. This helps identify and address potential security weaknesses before attackers can exploit them.
- Make sure to use both network and host-based monitoring tools and actively monitor relevant log messages for suspicious activities or anomalies. These tools should be able to identify and flag unauthorized access attempts, unusual traffic patterns, or unexpected system behaviors.

DETAILS AND RECOMMENDATIONS

2.5 Indicators of Attack Detected

Indicators of attack (IOAs) generally refer to a piece of evidence or a pattern that suggests an ongoing or imminent cyberattack. In the context of WatchGuard's Threat Hunting Service, IOAs are generated when there is a high probability of an attack. These attacks are typically at an early or exploitation stage and they do not generally use malware. Attackers commonly take advantage of legitimate operating system tools and hide their activity.

This table lists the most recent indicators of attack detected on your endpoints.

Latest IOA Detections

Endpoint	Indicator of Attack	Occurrences	Risk	Date
WIN-SERVER-2	LSASS process credential dumping using ProcDump	1	High	10/2/2023 12:42 AM
WIN-LAPTOP-1	Privilege escalation bypassing UAC	1	Critical	10/2/2023 12:29 AM
WIN-DESKTOP-1	File download via the svchost.exe process	4	Critical	10/2/2023 12:23 AM
WIN-DESKTOP-3	Execution of obfuscated command-line parameters using cmd.exe	5	Critical	10/2/2023 12:21 AM
WIN-DESKTOP-3	LSASS process credential dumping using PowerShell	1	Critical	10/2/2023 12:19 AM
WIN-SERVER-2	UAC bypass	6	Critical	10/1/2023 11:59 PM
WIN-SERVER-1	Exfiltration over network	5	High	10/1/2023 11:31 PM
WIN-SERVER-2	Disabling of Windows Defender with PowerShell	1	High	10/1/2023 10:07 PM
WIN-DESKTOP-1	Credentials compromised after brute-force attack on RDP	1	Critical	10/1/2023 9:27 PM
WIN-DESKTOP-1	UAC bypass	1	Critical	10/1/2023 9:15 PM
WIN-DESKTOP-1	Exfiltration over network	3	High	10/1/2023 8:17 PM
WIN-SERVER-2	Delete user account	2	Low	10/1/2023 2:13 PM
WIN-DESKTOP-2	Delete user account	1	Low	10/1/2023 8:29 AM
WIN-SERVER-1	Remote shares access	7	Medium	10/1/2023 4:35 AM
WIN-DESKTOP-3	Remote shares access	9	Medium	10/1/2023 12:12 AM
WIN-LAPTOP-1	Credentials compromised after brute-force attack on RDP	1	Critical	9/29/2023 11:27 PM
WIN-LAPTOP-1	In-memory execution of a remote script	1	Critical	9/29/2023 10:05 PM
WIN-LAPTOP-1	Use of pipes to escalate privileges	1	Critical	9/28/2023 12:03 AM
WIN-DESKTOP-3	Privilege escalation bypassing UAC	1	Critical	9/26/2023 10:29 PM
WIN-DESKTOP-3	Uninstallation of the WatchGuard endpoint protection	1	Medium	9/26/2023 9:19 PM

Recommendations

When an IOA is detected, verify whether it is an intrusion or a legitimate action or test. If the IOA is an intrusion, we recommend that you:

- Isolate the endpoint to contain the threat.
- Scan the endpoint.
- Change the endpoint credentials.
- Find the source of the execution to prevent the attack from occurring again.

DETAILS AND RECOMMENDATIONS

2.6 Actively Exploited Vulnerabilities Detected

Software vulnerabilities are flaws or weaknesses in software products, such as programming errors, design flaws, or memory safety violations that allow attackers to execute malicious code, install malware, or access sensitive data. While most published vulnerabilities are not being exploited “in the wild”, the availability of exploit code is an important factor to decide which patches should be prioritized for deployment.

This table lists vulnerabilities detected during the assessment that are actively being exploited. This means they are not only known, but also commonly used by hackers as a point of entry or as part of a toolset to move laterally in the network.

Latest Actively Exploited Vulnerability Detections

No Vulnerability Detections

Recommendations

It is important to understand which vulnerabilities pose a real and significant risk, based on factors such as severity, exploitability, impact, and exposure.

- Make sure to patch vulnerabilities as soon as possible to reduce the attack surface.
- Use automated methods to mitigate vulnerabilities at scale and in real time, as well as to detect future vulnerabilities through scanning and testing.
- Remove programs that are not actively in use to minimize the attack surface.

DETAILS AND RECOMMENDATIONS

2.7 Other Critical and Important Vulnerabilities

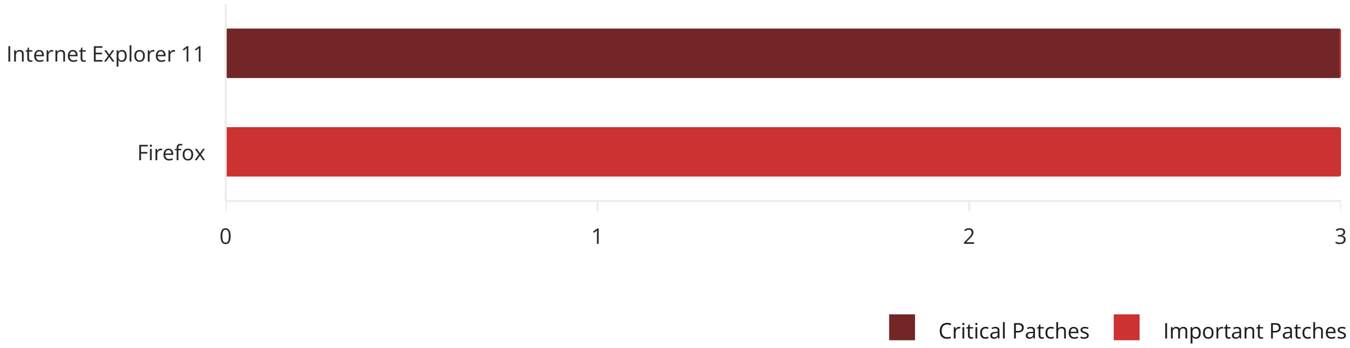
Over 80% of successful cyberattacks could have been prevented by applying software patches. In most cases, the required patches were available for more than 12 months before the attack took place.

This chart shows vulnerabilities detected during the assessment with a severity rating of Critical or Important:

- **Critical:** Vulnerability exploit could allow malware to spread without user interaction.

- **Important:** Vulnerability exploit could compromise the confidentiality, integrity, or availability of user data, or the integrity or availability of processing resources.

Top Programs with Critical and Important Vulnerabilities Detected



Recommendations

Deploying software patches is the single most effective risk mitigation strategy organizations can implement.

- Schedule recurrent vulnerability patching at least once a month to ensure consistency and reduce the time required to address security vulnerabilities.

- Dedicated patch management solutions or configuration management tools can help track vulnerabilities, prioritize patches, and automate deployment to keep all operating systems and software up to date.

DETAILS AND RECOMMENDATIONS

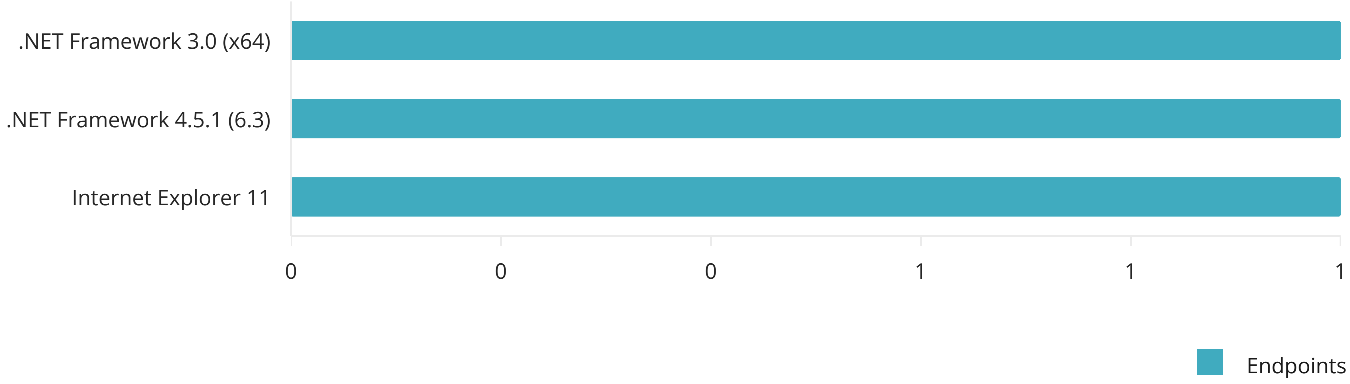
2.8 End-of-Life Software Detected

End-of-Life (EOL) software has reached the end of its support or maintenance period. This means the vendor no longer provides updates, bug fixes, and technical support for a specific version. The EOL stage usually occurs when software is considered outdated, not viable to support, or when vendor resources are focused on newer versions or entirely new products. EOL software is often used as an attack vector by attackers because it no longer receives critical security patches.

Because the presence of EOL software increases the organization\'s cybersecurity risk, it can also raise insurer concerns and affect cyber insurance terms, either by significantly limiting or excluding coverage altogether.

The assessment has identified that these endpoints have software programs installed that are already or will soon be in the EOL stage.

Most Common End-of-life Software Detected



Recommendations

EOL software could put your data and systems at risk, impacting your cybersecurity posture. It is important to stay up to date with software lifecycles and plan accordingly to ensure continued functionality, support, and security.

- Restrict the corporate software suite as much as possible to programs that are regularly patched.

- Uninstall any EOL software not in use.

DETAILS AND RECOMMENDATIONS

2.9 Applications with High Download Volume

Applications that receive an excessive amount of data can indicate that users are downloading undesired content or other applications. It can also be a symptom of failed updates or other routines which continually re-download data.

Applications with High Download Data Volume

No Applications

Recommendations

Applications with high download data volume can become security risks, introduce bandwidth usage issues, or reveal system misuse in general.

- Analyze the source and purpose of the excessive download data volumes. Understand whether it is related to normal business activities or data transfers, or if it indicates unauthorized or risky behavior.

- Deploy monitoring tools to proactively track and flag potential misuse.

- Identify high-volume endpoints or users to help pinpoint potential policy violations or identify compromised endpoints.

DETAILS AND RECOMMENDATIONS

2.10 Applications with High Upload Volume

Applications that upload a large amount of data can indicate system compromise, unauthorized data exfiltration attempts, or software malfunction. Excessive upload data volumes can also be a sign of policy violations or misuse of resources.

Applications with High Upload Data Volume

No Applications

Recommendations

Applications with high upload data volume can become security risks, introduce bandwidth usage issues, or reveal system misuse in general.

- Monitor upload data volumes to help identify unusual or suspicious data transfers that could be indicative of malicious activities, such as insider threats or external attackers attempting to steal sensitive information.

- Monitoring enables you to proactively detect and respond to potential security incidents, ensure compliance, protect sensitive information, optimize network usage, and maintain a robust security posture.

DETAILS AND RECOMMENDATIONS

2.11 LOTL applications executed

This section provides a list of executed applications that are not necessarily a risk, but could pose a security risk for different reasons. These Living-off-the-Land (LOTL) applications can include:

- **Tor or P2P (Peer-to-Peer) Sharing Clients**
  P2P sharing applications facilitate unauthorized download and sharing of illegal content and malicious files. The Tor network has the potential to anonymize malicious actions and illicit activities.

- **VPN Applications**
  To avoid exposing data to third-party providers that cannot be trusted, it is important to make sure that only corporate VPN or services otherwise validated by your organization are used. VPN software clients are often run by privileged accounts and outdated versions can introduce attack vectors that cybercriminals often use.

- **Cloud Storage Applications**
  It is important to control where data is stored geographically for compliance. Cloud services are also at risk of data exfiltration. When the cloud sync configuration keeps local copies of files by default, hardware loss or theft can become an issue.

- **Remote Connection Tools**
  Remote connection tools are a common attack vector. It is important to make sure that only approved and hardened remote connection and support tools are installed and used.

LOTL Applications

No LOTL Applications

Endpoints with LOTL Applications

No endpoints with LOTL Applications

Recommendations

Tor or P2P (peer-to-peer) sharing clients:

- Consider removing P2P sharing software from managed endpoints or actively monitoring data downloaded by these applications.
- Blocking access to Tor nodes and preventing Tor navigation can minimize the risk of exposure to cybercrime and malicious traffic.

VPN applications:

- Consider removing VPN software clients that are not validated by your organization.
- Implement checks to make sure that VPN-connected endpoints have a running endpoint security solution, and block access to the VPN if they do not.

Cloud storage applications:

- Consider enforcing policies when it comes to the use of cloud sync services, and the storage of personally identifiable information (PII) in company-approved cloud services.
- Monitor traffic to identify documents at risk of exfiltration.

Remote connection tools:

- Make sure to remove any remote tools not used by the organization to reduce the attack surface and harden the remote tools in use to prevent security risks.
- Tripwires and active monitoring can provide early insight on misuse or attack attempts.