# Task 3: **Perform a Basic Vulnerability Scan on Your PC.**

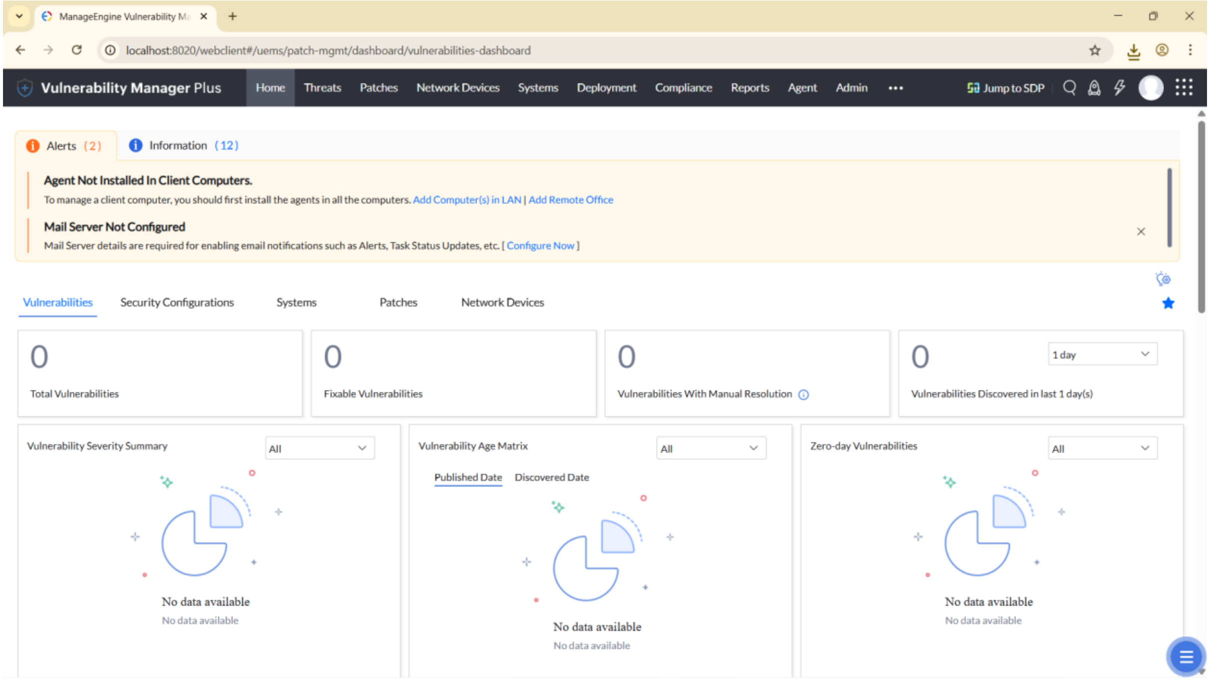
**BY: KUSH THAKER. (kthaker442@gmail.com)**

## Step 1,2,3,4: Getting a Vulnerability scanner and Scanning the Local-Host.

By default, as per the task I was assigned to install OpenVAS and Nessus.
As per my experience and proficiency, I am using ManageEngine's Vulnerability manager Plus as its Free to use and handy to use.

I Started the Vulnerability plus and scanned my personal PC (Name: Phoenix, OS: Windows 11).

Screenshots Pasted below.


ManageEngine Vulnerability M
localhost:8020/webclient#/uems/patch-mgmt/dashboard/vulnerabilities-dashboard
Vulnerability Manager Plus
Home
Threats
Patches
Network Devices
Systems
Deployment
Compliance
Reports
Agent
Admin
Jump to SDP
Alerts (2)
Information (12)

**Agent Not Installed In Client Computers.**
To manage a client computer, you should first install the agents in all the computers. Add Computer(s) in LAN | Add Remote Office

**Mail Server Not Configured**
Mail Server details are required for enabling email notifications such as Alerts, Task Status Updates, etc. [ Configure Now ]

0 Total Vulnerabilities

0 Fixable Vulnerabilities

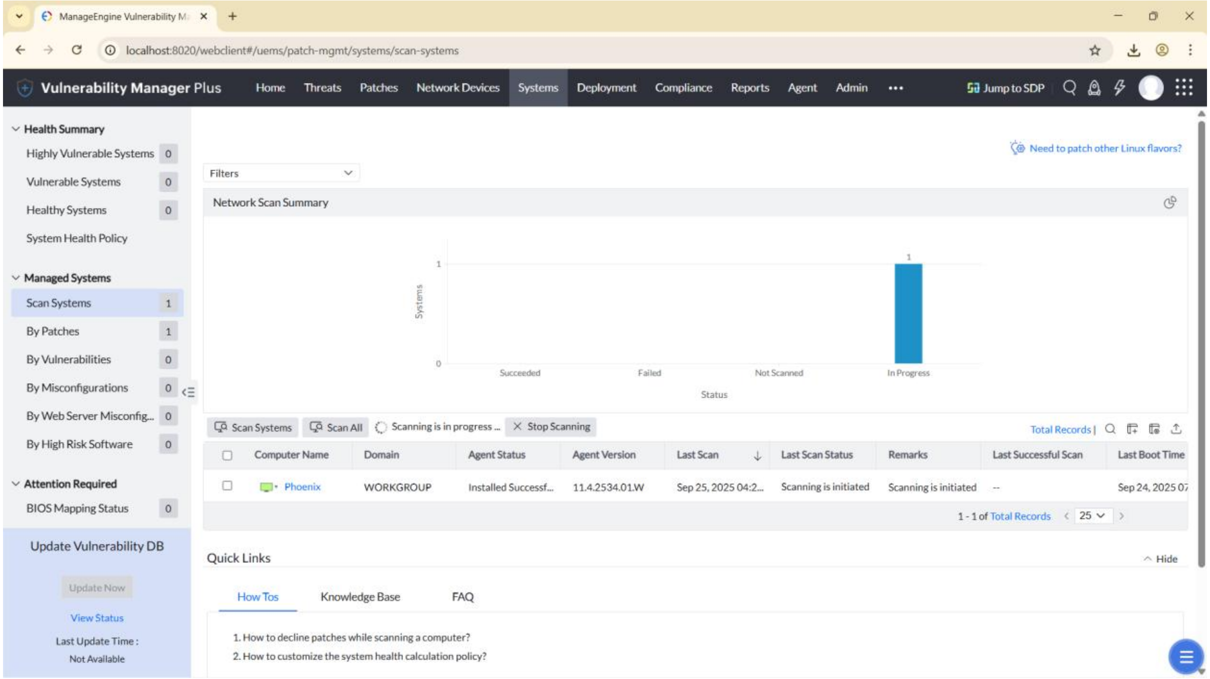
0 Vulnerabilities With Manual Resolution

0 Vulnerabilities Discovered in last 1 day(s) — 1 day

Vulnerability Severity Summary — All
No data available
No data available

Vulnerability Age Matrix — All
Published Date Discovered Date
No data available
No data available

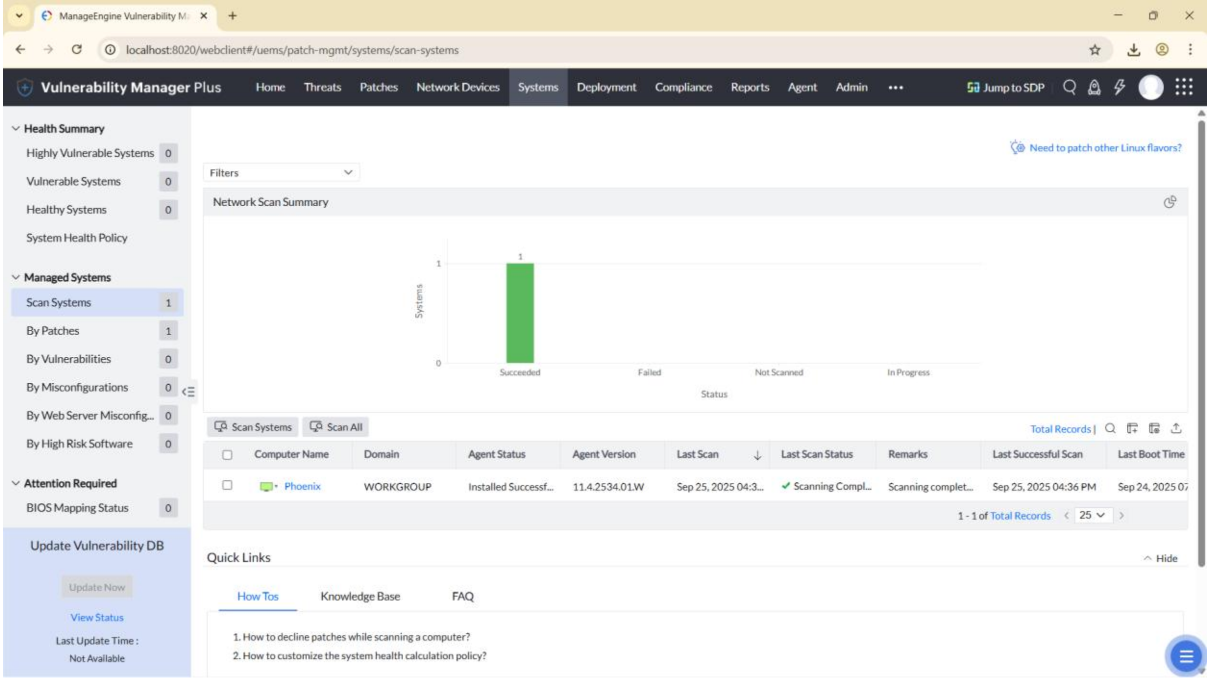
Zero-day Vulnerabilities — All
No data available
No data available



| ☐ | Computer Name | Domain | Agent Status | Agent Version | Last Scan | Last Scan Status | Remarks | Last Successful Scan | Last Boot Time |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | Phoenix | WORKGROUP | Installed Successf... | 11.4.2534.01.W | Sep 25, 2025 04:2... | Scanning is initiated | Scanning is initiated | -- | Sep 24, 2025 07 |

1 - 1 of Total Records 25

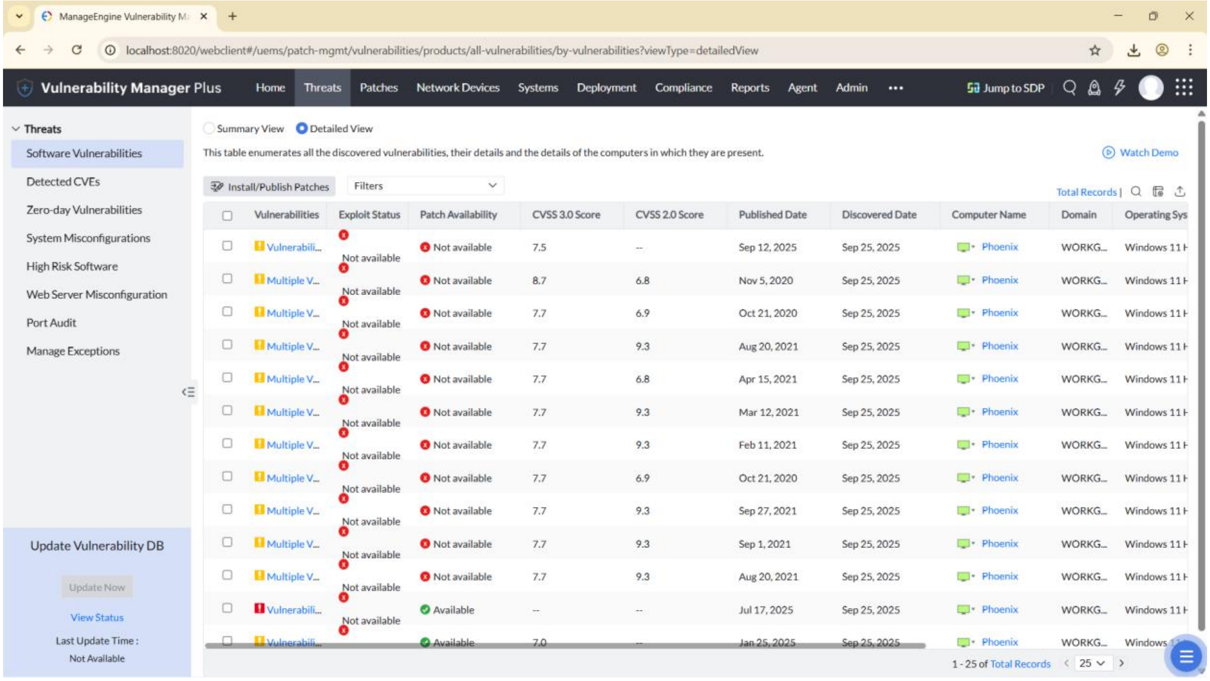
1. How to decline patches while scanning a computer?
2. How to customize the system health calculation policy?



| ☐ | Computer Name | Domain | Agent Status | Agent Version | Last Scan | Last Scan Status | Remarks | Last Successful Scan | Last Boot Time |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | Phoenix | WORKGROUP | Installed Successf... | 11.4.2534.01.W | Sep 25, 2025 04:3... | ✓ Scanning Compl... | Scanning complet... | Sep 25, 2025 04:36 PM | Sep 24, 2025 07 |

1 - 1 of Total Records 25

1. How to decline patches while scanning a computer?
2. How to customize the system health calculation policy?



This table enumerates all the discovered vulnerabilities, their details and the details of the computers in which they are present.

| □ | Vulnerabilities | Exploit Status | Patch Availability | CVSS 3.0 Score | CVSS 2.0 Score | Published Date | Discovered Date | Computer Name | Domain | Operating Sys |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Vulnerabili... | Not available | Not available | 7.5 | -- | Sep 12, 2025 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 8.7 | 6.8 | Nov 5, 2020 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 6.9 | Oct 21, 2020 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Aug 20, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 6.8 | Apr 15, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Mar 12, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Feb 11, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 6.9 | Oct 21, 2020 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Sep 27, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Sep 1, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Multiple V... | Not available | Not available | 7.7 | 9.3 | Aug 20, 2021 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Vulnerabili... | Not available | Available | -- | -- | Jul 17, 2025 | Sep 25, 2025 | Phoenix | WORKG... | Windows 11 H |
| □ | Vulnerabili... |  | Available | 7.0 | -- | Jan 25, 2025 | Sep 25, 2025 | Phoenix | WORKG... | Windows |

The **.pdf** and **.csv** file is already attacked to the repository's main branch.

## Step 5: Review the report for vulnerabilities and severity

After examining the Vulnerabilities, I have bifurcated them in 3 stages. **Critical, High and Medium.** As listed below.

| Software / Component | Vulnerability / CVEs | CVSS Score | Risk Level | Exploit Status | Patch Availability |
|---|---|---|---|---|---|
| **WinVerifyTrust** | **CVE-2013-3900 (Signature Validation)** | **8.7** | **High** | **Exploit available** | **Patch not available** |
| **Adobe Photoshop CC 21.2.1** | **Multiple Vulnerabilities** | **8.7** | **High** | **Not available** | **Not available** |
| **7-Zip 25.0.0 (x64)** | **CVE-2025-53816, CVE-2025-53817** | **–** | **–** | **Not available** | **Patch available (7z2501-x64.exe)** |
| **Adobe Photoshop 21.2.2** | **Multiple Vulnerabilities** | **7.7** | **High** | **Not available** | **Not available** |

| Software / Component | Vulnerability / CVEs | CVSS Score | Risk Level | Exploit Status | Patch Availability |
|---|---|---|---|---|---|
| WinRAR 7.12-beta1 (x64) | CVE-2025-8088 | – | – | Not available | Patch available (winrar-x64-7.13.exe) |
| Adobe Photoshop 21.2.10 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| Adobe Photoshop 21.9 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| Adobe Photoshop 21.2.8 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| WinRAR 6.99 (x64) | CVE-2024-33899, CVE-2024-36052 | 7.5 | High | Not available | Patch available (7.13) |
| VMware Workstation 17.6.3 | CVE-2025-22224, CVE-2025-22226 | 9.3 | Critical | Not available | Not available |
| Adobe Photoshop 21.2.4 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| VLC Media Player 3.0.20 (x64) | CVE-2024-46461 | 8.0 | High | Not available | Not available |
| Curl for Windows 8.16.0 | CVE-2025-10148, CVE-2025-9086 | 7.5 | High | Not available | Not available |
| Google Chrome 140.0.7339.x | CVE-2025-10890, CVE-2025-10891, CVE-2025-10892 | 9.1 | Critical | Not available | Patch available |
| Adobe Photoshop 21.2.0 | Multiple Vulnerabilities | 8.7 | High | Not available | Not available |
| Adobe Photoshop 21.2.9 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| MS Visual C++ 2015–2022 Redist (x64) | CVE-2024-43590 | 7.7 | High | Not available | Not available |
| WinRAR 7.12 (x64) | CVE-2025-8088 | – | – | Not available | Patch available (7.13) |

| Software / Component | Vulnerability / CVEs | CVSS Score | Risk Level | Exploit Status | Patch Availability |
|---|---|---|---|---|---|
| Adobe Photoshop 21.2.6 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| VMware Workstation 17.6.3 | CVE-2025-41225, CVE-2025-41226, CVE-2025-41227, CVE-2025-41228 | 8.8 | High | Not available | Patch available |
| 7-Zip 24.07 (x64) | CVE-2024-11477 | 7.7 | High | Not available | Patch available |
| VLC Media Player 3.0.18 (x64) | CVE-2023-46814 | 7.7 | High | Not available | Patch available |
| VLC Media Player 3.0.19 (x64) | CVE-2023-47359, CVE-2023-47360 | 9.8 | Critical | Not available | Patch available |
| Adobe Photoshop 21.2.5 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |
| 7-Zip 24.08 (x64) | CVE-2024-11612 | 6.4 | Medium | Not available | Patch available |
| 7-Zip 24.09 (x64) | CVE-2025-0411 | 7.0 | High | Not available | Patch available |
| VLC Media Player 3.0.10 (x64) | CVE-2020-13428 | 7.7 | High | Not available | Patch available |
| WinRAR 7.11 (x64) | CVE-2025-6218 | 7.8 | High | Not available | Patch available |
| WinRAR 7.10 (x64) | CVE-2025-31334 | 6.8 | Medium | Not available | Patch available |
| Adobe Photoshop 21.2.11 | Multiple Vulnerabilities | 7.7 | High | Not available | Not available |

PTO.

The vulnerability scan revealed a wide range of security issues across critical applications such as **VMware Workstation, Google Chrome, VLC Media Player, WinRAR, 7-Zip, Microsoft Visual C++ Redistributables, and Adobe Photoshop**. The findings include several **critical vulnerabilities (CVSS 9.8–9.1)**, many **high-severity issues**, and a smaller number of **medium-risk weaknesses**. Some of these, like the **WinVerifyTrust flaw (CVE-2013-3900)**, already have known exploits in circulation, which increases their urgency.

While patches are available for most of the affected software (e.g., **WinRAR, 7-Zip, VLC, Chrome, and VMware**), others like older versions of **Adobe Photoshop** remain unsupported and vulnerable without an upgrade path.

We will now move forward with **in-depth research into these vulnerabilities**, examining their potential impact, vendor advisories, patch availability, and practical mitigation steps to prioritize remediation effectively.

Now let’s Jump into step 6 about their fixes and mitigations. Though I don’t want to mitigate. I will keep them as it is and just research and inform you about those securities.

## Step 6: Fixing and Mitigating Critical Vulnerabilities.

I didn’t mitigate but researched About them (**Note: THIS ARE ONLY CRITICAL VULN…….**). The research is written below about their Nature and mitigations.

**1. WinVerifyTrust (CVE-2013-3900)**

- **Nature of Vulnerability:** This flaw exists in the **WinVerifyTrust signature validation function**, which can allow attackers to bypass security checks by crafting maliciously signed executables. Because the exploit is already known, it presents an **active risk of malware delivery**.
- **Mitigation Steps:**
    1. Apply Microsoft’s official **registry-based workaround** by enabling the padding check:
        - Create or update the DWORD key EnableCertPaddingCheck=1 under HKLM\Software\Microsoft\Cryptography\Wintrust\Config.
    2. Install the relevant **KB security patch** from Microsoft (if available for your OS version).
- **Essence:** Since this is an old but still dangerous flaw, applying the registry change is the minimum safeguard, but patching is strongly preferred where possible.

**2. Adobe Photoshop 21.x (Multiple CVEs)**

- **Nature of Vulnerability:** Older releases of **Photoshop CC 21.x** contain multiple critical vulnerabilities, including memory corruption and arbitrary code execution flaws. Adobe has **retired these versions**, meaning no new patches are issued.
- **Mitigation Steps:**
  1. **Immediate upgrade** to the latest **Adobe Creative Cloud (2025 release)**.
  2. For environments where upgrading is delayed, **restrict file input sources** (e.g., do not open untrusted PSDs or images).
- **Essence:** The only realistic and secure path forward is migration to supported builds — running outdated Adobe software leaves permanent exposure.

**3. 7-Zip (CVE-2024-11477, CVE-2024-11612, CVE-2025-0411, CVE-2025-53816/53817)**

- **Nature of Vulnerability:** Multiple flaws exist in **7-Zip**, ranging from heap buffer overflows to extraction path traversal issues. These can allow attackers to execute arbitrary code or escalate privileges simply through malicious archive files.
- **Mitigation Steps:**
  1. Download and install **7-Zip 25.01 (x64)**, which addresses all currently known CVEs.
  2. If updating immediately is not possible, **disable file association** for 7-Zip and use it only on trusted archives.
- **Essence:** Updating 7-Zip is low-effort but highly impactful — a classic case where patching is the simplest, strongest protection.

**4. WinRAR (CVE-2024-33899, CVE-2024-36052, CVE-2025-8088, CVE-2025-6218, CVE-2025-31334)**

- **Nature of Vulnerability:** WinRAR is historically notorious for archive parsing flaws. These CVEs range from **buffer overflows** to **malicious ACE/RAR extraction exploits**. Some allow **remote code execution** when extracting crafted archives.
- **Mitigation Steps:**
  1. Update to **WinRAR 7.13** (winrar-x64-7.13.exe). This release fixes all five reported CVEs.
  2. In corporate environments, apply **group policy restrictions** to prevent execution of unpatched WinRAR versions.
- **Essence:** Because attackers commonly weaponize archive files, leaving WinRAR outdated is like leaving the front door unlocked. Update is mandatory.

**5. VMware Workstation (CVE-2025-22224, CVE-2025-22226, CVE-2025-41225–41228)**

- **Nature of Vulnerability:** These flaws affect **VMware Workstation 17**, primarily allowing **guest-to-host escapes** and **privilege escalations**. CVSS scores range from **8.8 to 9.3**, marking them as near-critical for virtualization-heavy environments.
- **Mitigation Steps:**
    1. Upgrade to **VMware Workstation 17.6.4** (VMware-workstation-full-17.6.4-24832109.exe).
    2. Some CVEs (notably CVE-2025-41225–41228) may require **manual patch uploads** from VMware's site.
    3. As a defense-in-depth measure, limit exposure by **restricting untrusted VM images** and **isolating host networks**.
- **Essence:** Given VMware's role as a hypervisor, exploitation could collapse isolation layers — upgrading is business-critical, not optional.

**6. VLC Media Player (CVE-2020-13428, CVE-2023-46814, CVE-2023-47359/47360, CVE-2024-46461)**

- **Nature of Vulnerability:** VLC vulnerabilities typically allow **remote code execution** through crafted video files. The 2023–2024 CVEs include **heap corruption** and **integer overflow** exploits, some with critical CVSS ratings (up to 9.8).
- **Mitigation Steps:**
    1. Update to **VLC 3.0.21** (vlc-3.0.21-win64.exe).
    2. Until patched, avoid opening **unverified or pirated media files**, as they are the most common attack vector.
- **Essence:** VLC is widely used, and "malicious movie files" have historically been effective attack payloads. Updating should be prioritized.

**7. CURL for Windows (CVE-2025-10148, CVE-2025-9086)**

- **Nature of Vulnerability:** These vulnerabilities affect **CURL's handling of HTTP/HTTPS requests**, allowing **denial-of-service** and potential **data leaks** under certain conditions.
- **Mitigation Steps:**
    1. Upgrade to **CURL 8.16.0+**.
    2. For servers relying on CURL scripts, implement **input validation** to reduce exposure to malicious endpoints.
- **Essence:** While not as immediately devastating as RCE flaws, CURL vulnerabilities can undermine data integrity in automated pipelines — patching is the safer bet.

**8. Google Chrome (CVE-2025-10890, CVE-2025-10891, CVE-2025-10892)**

- **Nature of Vulnerability:** These are **zero-day Chrome vulnerabilities**, typically involving **V8 JavaScript engine exploits** and **sandbox escapes**. Attackers can chain these flaws for full system compromise.
- **Mitigation Steps:**
    1. Update to the latest **Chrome 140.0.7339.208 or later** (googlechromestandaloneenterprise64_140.0.7339.208.msi).
    2. Enable **automatic Chrome updates** to ensure future zero-days are patched quickly.
- **Essence:** Given Chrome's ubiquity, this is one of the most dangerous categories — attackers heavily target browsers due to their constant exposure.

**9. Microsoft Visual C++ Redistributable (CVE-2024-43590)**

- **Nature of Vulnerability:** This affects the **runtime libraries** shipped with MS Visual C++. Exploits may allow **memory corruption** in applications that depend on these redistributables.
- **Mitigation Steps:**
    1. Install the updated redistributable **14.40.33816 or newer**.
    2. Verify that applications running on the system correctly load the patched version.
- **Essence:** It's easy to overlook runtime libraries, but unpatched redistributables can silently compromise every app that depends on them.

**PTO.**

# Step 7 — Full documentation of the most critical vulnerabilities.

**1) VLC Media Player — CVE-2023-47359 / CVE-2023-47360**

**CVSS:** 9.8 — **Risk Level:** Critical
**Found in scan:** VLC Media Player 3.0.19 (x64)

**Summary / Description**

Two high-severity vulnerabilities in VLC allow remote code execution when a user opens a specially crafted media file. These vulnerabilities stem from flaws in the media file parsing/decoding logic (heap corruption / integer overflow), enabling an attacker to execute arbitrary code with the privileges of the user running VLC.

**Attack Vector & Impact**

- **Vector:** A victim must open or preview a maliciously crafted media file (local file, or streamed via a malicious site or emailed attachment).
- **Impact:** Remote code execution in user context → full compromise of the desktop session; could be used to persist, exfiltrate data, or move laterally.

**Affected Versions (per scan)**

- VLC Media Player 3.0.19 (x64) and older 3.0.x builds noted in the report (3.0.18, 3.0.20 etc.)

**Exploit / Patch Status (per uploaded report)**

- **Exploit status:** Not listed as “exploit available” in the scan output, but CVSS and historical behavior make this highly exploitable.
- **Patch availability:** Patch available — update to **VLC 3.0.21 (win64)** as listed in report.

**Remediation (recommended)**

**Immediate (0–24 hrs):**

1. Block untrusted file vectors: prevent users from opening media from untrusted sources; temporarily disable automatic media previews in email clients and file managers.
2. Restrict execution rights where possible (use AppLocker/Windows App Control to restrict running of non-approved media players).
3. For high-risk users (admins, developers), temporarily remove VLC until patched.

**Definitive (24–72 hrs):**

1. Deploy VLC 3.0.21 to all affected hosts. Use the vendor installer referenced in the scan (vlc-3.0.21-win64.exe).

2. Apply via endpoint management (SCCM/Intune/WSUS packaging) and ensure restart where required.

**Long-term:**

- Enforce application inventory and update policy for all user-facing media apps. Consider using hardened players / sandboxing for untrusted media.

**Validation / Verification**

- After patching, confirm version 3.0.21 on hosts (Registry or About in UI, or vlc --version on command line).
- Test by scanning an updated host with the same scanner and verify the specific CVEs no longer appear.
- Check EDR/AV telemetry for any prior exploitation indicators (suspicious child processes launched by vlc.exe).

**Priority & Owner**

- **Priority:** P0 / Critical — immediate remediation required for all user systems.
- **Owner:** Endpoint/IT Operations for deployment; Security for monitoring and hunting.

**Rollback/Contingency**

- If the new build causes compatibility issues with custom codecs, isolate affected hosts and use a sandboxed player until a workaround or vendor patch addresses the codec problem.

**2) VMware Workstation — CVE-2025-22224, CVE-2025-22226, CVE-2025-41225–41228**

**CVSS:** up to 9.3 — **Risk Level:** Critical / High
**Found in scan:** VMware Workstation 17.6.3

**Summary / Description**

Multiple high-to-critical vulnerabilities in VMware Workstation 17 allow an attacker to escape from a guest to the host (guest-to-host escape) or perform privilege escalation. These issues compromise VM isolation — a central security boundary in virtualized environments.

**Attack Vector & Impact**

- **Vector:** Malicious code executed inside a VM (e.g., attacker-controlled guest image, compromised user VM) triggers a bug in the virtualization stack to execute code on the host or escalate privileges.
- **Impact:** Host compromise, compromise of other VMs, loss of isolation, potential full environment takeover.

**Affected Versions (per scan)**

- VMware Workstation 17.6.3 (and specific 17.x builds referenced in the report)

**Exploit / Patch Status (per uploaded report)**

- **Exploit status:** Not shown as “exploit available” in scan, but severity and CVSS imply strong risk in virtualization setups.
- **Patch availability:** Update available — **VMware Workstation 17.6.4**; some fixes require manual upload/install per vendor notes.

**Remediation (recommended)**

**Immediate (0–12 hrs):**

1. Restrict use of untrusted or public VM images. Remove unvetted VMs from hosts.
2. Isolate hosts running Workstation from critical networks (segmentation) until patched.

**Definitive (12–72 hrs):**

1. Apply **VMware Workstation 17.6.4** on all affected hosts. Follow vendor guidance for manual patch uploads where required.
2. Ensure host OS and virtualization components are fully patched; verify signatures and checksums of updates.

**Long-term:**

- Move production VMs to server-class hypervisors (vSphere/ESXi) with stricter patch processes when appropriate. Enforce least-privilege access to host systems and use host-based EDR.

**Validation / Verification**

- Post-install, confirm version 17.6.4 on Workstation hosts.
- Re-run the scanner and ensure the specific CVE entries are cleared.
- Search EDR/host logs for unusual VM escape indicators (unexpected vmware service restarts, new processes launched by VM processes, suspicious network connections originating from host VM management services).

**Priority & Owner**

- **Priority:** P0 / Critical for hosts that run untrusted VMs or developer/testing laptops; P1 for other hosts.
- **Owner:** Virtualization/IT Operations for patch deployment; Security for host monitoring.

**Rollback/Contingency**

- Keep backups of VMs and host snapshots before broad patching. Have a rollback plan if the patch causes regressions, but weigh rollback risk vs. exposure to a guest-to-host escape.

### 3) Google Chrome — CVE-2025-10890, CVE-2025-10891, CVE-2025-10892

**CVSS:** 9.1 — **Risk Level:** Critical
**Found in scan:** Google Chrome 140.0.7339.x

**Summary / Description**

A trio of high-severity Chrome vulnerabilities (likely affecting the V8 engine, rendering, or sandbox escape) can be chained to achieve remote code execution and break browser sandboxing. These are typical "browser zero-day" classes: high impact because browsers are frequently exposed.

**Attack Vector & Impact**

- **Vector:** Drive-by download or malicious web content (or malicious attachment) leading to exploitation through the browser.
- **Impact:** Arbitrary code execution on user systems, data theft, credential theft, lateral movement.

**Affected Versions (per scan)**

- Google Chrome 140.0.7339.207/208 (older patched builds flagged in report)

**Exploit / Patch Status (per uploaded report)**

- **Exploit status:** Not marked as exploited in the scan, but browser zero-days are commonly weaponized quickly.
- **Patch availability:** Patch is available — upgrade to **Chrome 140.0.7339.208** (standalone enterprise MSI referenced in the report).

**Remediation (recommended)**

**Immediate (0–6 hrs):**

1. Enforce browser update policies to push Chrome 140.0.7339.208 immediately.
2. For managed endpoints, enable auto-updates and force-restart where needed.

**Definitive (6–24 hrs):**

1. Deploy the enterprise MSI across endpoints via management tools.
2. Consider blocking access to risky sites, and temporarily restrict use of browser extensions from untrusted sources.

**Long-term:**

- Employ browser isolation for high-risk users, and use endpoint protection to block exploit behavior (memory exploitation, code injection).

**Validation / Verification**

- Confirm Chrome version 140.0.7339.208+ on endpoints.
- Verify via central update logs / GPO that the update was applied.

- Review browser-related telemetry for suspicious exploitation behavior (unusual child processes, use of debugging APIs, or crash reports correlated to pre-patch exploits).

**Priority & Owner**

- **Priority:** P0 / Critical — browsers are high exposure.
- **Owner:** Endpoint Management for deployment; Security for monitoring and web-proxy blocking.

**Rollback/Contingency**

- If update breaks enterprise apps, isolate those users and use whitelisting/testing before rolling out to all users.

**4) WinVerifyTrust — CVE-2013-3900 (Signature Validation)**

**CVSS:** 8.7 — **Risk Level:** High (legacy but exploited)
**Found in scan:** WinVerifyTrust Signature Validation Vulnerability

**Summary / Description**

This is a legacy but serious vulnerability in Windows' signature verification routine (WinVerifyTrust). An attacker can craft signed files that bypass signature validation, enabling execution of apparently "signed" malicious binaries. Because it undermines code-signing trust, it can be leveraged to distribute malware that appears legitimate.

**Attack Vector & Impact**

- **Vector:** Delivery of a maliciously crafted signed executable (via email, download, or removable media).
- **Impact:** Execution of malicious code appearing to be signed by a legitimate publisher; can bypass some security controls that trust signed code.

**Affected Versions (per scan)**

- Windows systems where WinVerifyTrust behavior is unpatched / default.

**Exploit / Patch Status (per uploaded report)**

- **Exploit status: Exploit available** per scan — real-world exploitation has occurred.
- **Patch availability:** Patch not available for some older platforms per scan; vendor has historically provided KB/workarounds.

**Remediation (recommended)**

**Immediate (0–12 hrs):**

1. Implement Microsoft's registry workaround: set EnableCertPaddingCheck=1 under HKLM\Software\Microsoft\Cryptography\Wintrust\Config (test on a few hosts first).
2. Block execution of unsigned or untrusted binaries via AppLocker or equivalent.

**Definitive (24–72 hrs):**

1. Apply Microsoft official patch/KB if applicable to your OS (check Microsoft Security Advisories for your OS build).
2. Enforce stricter execution policies: block running executables from user-writable paths (Downloads, Temp), and restrict code signing trust to enterprise PKI where possible.

**Long-term:**

- Use endpoint protection that verifies binary reputation and performs deep scanning even for signed binaries.

**Validation / Verification**

- Validate registry setting presence and effect on a test host.
- Monitor SIEM for attempts to execute binaries with suspicious signatures or from untrusted folders.
- Re-run scanner to confirm WinVerifyTrust vulnerability is no longer flagged.

**Priority & Owner**

- **Priority:** P0 / High — because exploit exists and it undermines signature protections.
- **Owner:** Endpoint/Windows Systems team for registry/patch deployment; Security for policy enforcement.

**Rollback/Contingency**

- Changing signature validation behavior might cause compatibility issues with legitimate signed software; test widely before enterprise-wide rollout and be ready to revert registry changes if critical business apps break — but pair rollback with alternate mitigations (AppLocker rules) to avoid leaving hosts unprotected.

**5) (Honorable mention) WinRAR / 7-Zip family (multiple CVEs aggregated)**

**CVSS:** generally 7.0–7.8 (multiple entries) — **Risk Level:** High / Medium
**Found in scan:** WinRAR (various versions), 7-Zip (24.x/25.x)

**Summary / Description**

Multiple archive-handling vulnerabilities (buffer overflows, path traversal, parsing errors) that allow arbitrary code execution when extracting or previewing malicious archives. Because compressed files are a common delivery mechanism (email attachments, downloads), these are high-risk for desktop users.

**Attack Vector & Impact**

- **Vector:** Opening or extracting a specially crafted archive (RAR, 7z, etc.).
- **Impact:** Remote code execution in the context of the user; potential privilege escalation if combined with other flaws.

**Affected Versions (per scan)**

- Various: WinRAR 6.99, 7.10, 7.11, 7.12, and 7z versions 24.07/24.08/24.09/25.0.0 as noted.

**Exploit / Patch Status (per uploaded report)**

- **Exploit status:** Not explicitly marked as exploited in the scan; known to be actively targeted historically.
- **Patch availability:** Patches available — update to **WinRAR 7.13** and **7-Zip 25.01** as referenced.

**Remediation (recommended)**

**Immediate:**

1. Educate users to NOT extract archives from untrusted sources. Disable automatic file association where possible.
2. Use EDR to block suspicious extraction behavior (child processes spawned by archive programs that drop executables into Startup folders, etc.)

**Definitive:**

1. Upgrade to WinRAR 7.13 and 7-Zip 25.01 across the environment via endpoint management.

**Validation / Verification**

- Confirm updated versions via software inventory and by rescanning.

**Priority & Owner**

- **Priority:** P1 — High-priority for desktops and file-handling servers.
- **Owner:** Endpoint & Desktop Ops.

# Summary:

I performed a **basic vulnerability scan** on my Windows 11 PC using **ManageEngine Vulnerability Manager Plus**, analysed the results, and categorized vulnerabilities as Critical, High, or Medium. The scan revealed risks in applications like **VMware Workstation, Google Chrome, VLC Media Player, WinRAR, 7-Zip, Adobe Photoshop, CURL, and MS Visual C++**, including some actively exploitable flaws. While I did not mitigate them, I researched each critical issue, understood their nature, impact, and recommended fixes, gaining hands-on knowledge of vulnerability assessment, risk classification, and software security management.

**Regards,**

**KUSH THAKER.**