

● Vulnerability scan

Vulnerability Scan

Practice name removed

Software vulnerability check: one front-desk computer

PREPARED FOR

Practice name removed

PREPARED BY

Chuck Weiselberg, One Guy
Consulting

DATE

10-21-2026

CONTENTS

In this report

01	What we found The bottom line, the count at each priority, and what this assessment is and is not.	03
02	Risk posture Where things stand, and how we set priority.	04
03	What the findings map to Each finding matched to the HIPAA Security Rule safeguard it relates to, with the reason.	06
04	Findings that need action 5 finding cards, most urgent first: what each is, why it matters, what to do.	07
05	Strengths: none assessed None assessed: this check looked for weaknesses only.	12
06	Software inventory The installed programs Wazuh listed, and what this check could not see.	12
07	What to do, in order 5 steps, one per fix, most urgent first: who does each and how you know it is done.	12
08	How this assessment was made The tools and versions, when we tested, the authorization, Coverage and the Evidence register.	14

— THE BOTTOM LINE

01 What we found

Five programs on this computer are out of date. Three have flaws attackers have been seen using, and our check matched each to the installed version and part: 7-Zip 19.00, Mozilla Firefox 115.0 and Adobe Acrobat Reader 23.006.20320. The other two have published flaws that still need fixing: Notepad++ 8.5.6 and VLC media player 3.0.11. Section 07 lists the steps, most urgent first. Section 08 lists what was and was not checked.

3

CRITICAL

Fix now. Highest-priority exposure.

2

FIX SOON

Worth fixing this cycle.

0

ROUTINE

Low priority. Review each one, then fix it in normal maintenance if it applies.

WHAT THIS ASSESSMENT IS

- A check of the installed software on one practice computer, and the known flaws that affect it.
- One front-desk computer running Windows 11 Pro, checked through the Wazuh agent installed on it. This computer is in One Guy Consulting's own test office and was set up with older versions of common office software. It is not a client's computer. Names are removed.
- Evidence for the practice's HIPAA risk analysis and risk management; section 03 explains how.

WHAT IT IS NOT

- Not the full risk analysis. Administrative and physical safeguards, policies and workforce are separate.
- Not a scan of your wider network. A network assessment does that.
- Not a guarantee that no other flaws exist. A scan finds only what its checks look for.
- Not a compliance certification.
- Real client reports are confidential. We deliver them through the client portal or as an encrypted file, never by unencrypted email.

OBSERVED POSTURE

02 Risk posture

OBSERVED POSTURE

Action required

Five programs are out of date, and three have flaws attackers have been seen using. Updating or removing them, then confirming it with a recheck, closes the findings in this report.

A retest of each finding after its fix is your before-and-after proof.

How we set priority. Priority is the order to fix things in. Each flaw has a public ID number (its CVE) and a severity score from 0 to 10 published in NVD, the U.S. government's National Vulnerability Database. The score says how bad a flaw is in general, not whether it can be used on this computer, so the score alone does not set priority. Wazuh, the free security software that ran on this computer, reported what is installed.

Evidence and validation states. Each one establishes a different fact:

- **Observed:** a fact we saw ourselves, such as a program and its version read from the computer.
- **Scanner match (version match):** Wazuh's feed says published flaws affect that version. The flaw could apply here; nobody has reviewed it one by one.
- **Analyst-confirmed:** we checked one flaw against the vendor's advisory: the installed version is in the affected range and the vulnerable part is present. That is not proof it can be used here. Section 08 shows each check.
- **Exploited:** we made the flaw work here. We did not try, so nothing in this report is in this state.

Every finding in this report is a version match, and a version match is Fix soon. Two things raise the urgency. First, a flaw on CISA's Known Exploited Vulnerabilities list, so attackers have been seen using it: if our check matches it to this computer (the vendor's affected versions include what is installed, and the vulnerable part is present), that finding is Critical. Second, a Fix soon finding whose published score is 9.0 or higher gets a 2-week target instead of 30 days. Critical here means fix first. It is a priority, not a measured business impact: we did not assess how often a program is used, what the user is allowed to do on the computer, or other protections that may lower the risk.

The table below shows these rules. If two sources ever disagree, we look into it, and until that is settled the finding keeps the higher priority. We can move a finding off its default priority, but only with the reason recorded against the finding, and the "Why" line on its card shows any such override.

DEFAULT RULES	CRITICAL	FIX SOON	ROUTINE
Wazuh The tool's own rating.	A flaw in the installed version is on CISA's Known Exploited Vulnerabilities list (known exploited) and our check matched the installed version and part	Any other installed program version that published flaws affect (2-week target at a published score of 9.0 or higher)	Not used in a software check

— BY HIPAA SAFEGUARD

03 What the findings map to

Each finding is matched to the HIPAA Security Rule safeguard it relates to. A match does not mean ePHI (electronic protected health information) was exposed. This sample computer holds no ePHI. On a real front-desk computer, these programs would sit alongside patient records. How to use these results: record each finding in the practice's risk analysis (45 CFR 164.308(a)(1)(ii)(A)) as a known weakness on a computer that can reach patient data, with CISA's list as evidence that attacks are likely. Then track the fixes in section 07, with owners, dates and evidence, as part of risk management (45 CFR 164.308(a)(1)(ii)(B)). Neither step alone establishes compliance.

SAFEGUARD	CITATION	CRITICAL	FIX SOON	ROUTINE
Risk Management Keeping installed software patched is one of the security measures that keep risks to a reasonable level.	45 CFR 164.308(a)(1)(ii)(B)	3	2	0

— IN PLAIN ENGLISH

04 Findings that need action

◆ CRITICAL

Outdated Software: 7-Zip 19.00

WAZUH AGENT

HIPAA Risk Management · 45 CFR 164.308(a)(1)(ii)(B)

What it is: This computer has 7-Zip 19.00 installed. One of its flaws is on CISA's list of flaws attackers have been seen using (CVE-2025-0411); we reviewed it by hand. Scanner data: Wazuh's feed matches 15 unique flaw IDs (CVEs) to this version by its version number, not reviewed one by one. The highest-rated, CVE-2026-48095, scores 8.8 out of 10. NVD marks 1 more as disputed, so we leave it out.

Why it matters: Compressed files (.zip, .7z) are a common way attackers hide malware in email attachments. A known flaw in the tool that opens them can let a crafted file run code or slip past Windows' download warnings.

Why Critical: CVE-2025-0411 is on CISA's Known Exploited Vulnerabilities list, so attackers have been seen using it, and our check matched it to the installed version and the vulnerable part. NVD and 7-Zip's own release history put the fix in 24.09. This computer has 19.00; the attacker needs the user to extract a crafted archive with 7-Zip.

What we confirmed: The Wazuh agent read the version from the computer's list of installed software, and its server matched it against published flaw lists. We checked the CISA-listed flaw against the maker's advisory (table in section 08). On the computer we found the vulnerable part installed (component check, section 08). We did not test whether any flaw can be used here.

Evidence (section 08): E01 (Wazuh agent), E02 (OGC check), E03 (OGC capture).

WHAT TO DO

Download the current version from 7-zip.org and install it over the old one. 7-Zip does not update itself, so add it to the practice's regular update list. If no one at the practice uses it, uninstall it instead.

ID OGC-DDS-F01 INSTALLED AS 7-Zip 19.00 (x64) FLAWS SHOWN: 3 OF 15 CVE-2025-0411

CVE-2026-48095 CVE-2026-48092 CISA: known exploited, version and part match

◆ CRITICAL

Outdated Software: Mozilla Firefox 115.0

WAZUH AGENT

HIPAA Risk Management · 45 CFR 164.308(a)(1)(ii)(B)

What it is: This computer has Mozilla Firefox 115.0 installed. Three of its flaws are on CISA's list of flaws attackers have been seen using (CVE-2024-9680, CVE-2023-5217 and CVE-2023-4863); we reviewed each by hand. Scanner data: Wazuh's feed matches 912 unique flaw IDs (CVEs) to this version by its version number, not reviewed one by one. Its highest-rated flaws score 10.0 out of 10.

Why it matters: A web browser touches the internet all day. A booby-trapped web page or ad can use a known browser flaw to run an attacker's code on this computer, with access to everything the user can open, including patient records and the practice's email.

Why Critical: CVE-2024-9680, CVE-2023-5217 and CVE-2023-4863 are on CISA's Known Exploited Vulnerabilities list, so attackers have been seen using them, and our check matched each to the installed version and the vulnerable part. Mozilla fixed CVE-2024-9680 in Firefox 131.0.2; the attacker needs the user to open web content built to trigger it. Mozilla fixed CVE-2023-5217 in 118.0.1 (a crafted VP8 video stream) and CVE-2023-4863 in 117.0.1 (a crafted WebP image); CISA files these two under Google Chromium, and Mozilla's advisories confirm Firefox is affected.

What we confirmed: The Wazuh agent read the version from the computer's list of installed software, and its server matched it against published flaw lists. We checked the CISA-listed flaws against the maker's advisory (table in section 08). On the computer we found the vulnerable part installed (component check, section 08). We did not test whether any flaw can be used here.

Evidence (section 08): E01 (Wazuh agent), E02 (OGC check), E03 (OGC capture).

WHAT TO DO

Remove the Windows policy that blocks Firefox updates (DisableAppUpdate, found on this computer), then update Firefox and check its automatic updates are on (Settings, General, Firefox Updates). If no one at the practice uses it, uninstall it instead.

ID OGC-DDS-F02 INSTALLED AS Mozilla Firefox (x64 en-US) 115.0 FLAWS SHOWN: 3 OF 912

CVE-2024-9680

CVE-2023-5217

CVE-2023-4863

CISA: known exploited, version and part match

◆ CRITICAL

Outdated Software: Adobe Acrobat Reader 23.006.20320

OGC VERSION CHECK

HIPAA Risk Management · 45 CFR 164.308(a)(1)(ii)(B)

What it is: This computer has Adobe Acrobat Reader 23.006.20320 installed, a version from September 2023. Adobe has released many security updates since then, and NVD lists 155 published flaws that affect this version, including one on CISA's list.

Why it matters: PDF files arrive by email from patients, labs and insurers. A booby-trapped PDF can use a known reader flaw to take over the computer when someone opens it.

Why Critical: CVE-2026-34621 is on CISA's Known Exploited Vulnerabilities list, so attackers have been seen using it, and our check matched it to the installed version and the vulnerable part. Adobe's bulletin APSB26-43 says Reader versions up to 26.001.21367 are affected and that Adobe knows of attacks using it; the fix is 26.001.21411. This computer has 23.006.20320; the attacker needs the user to open a crafted PDF in Reader.

What we confirmed: The Wazuh agent listed Adobe Acrobat Reader 23.006.20320 on this computer, but Wazuh's vulnerability feed flagged nothing for it. We checked it by hand and with NVD: NVD's affected versions include this version for 155 published flaws (17 from 2023, 53 from 2024, 25 from 2025, 60 from 2026), because this copy has missed three years of Adobe updates. One of them, CVE-2026-34621, is on CISA's list; Adobe's bulletin APSB26-43 confirms it affects this version. The other Acrobat Reader flaws on CISA's list (catalog dated 10-16-2026) were fixed earlier or in this version. On the computer we found the vulnerable part installed (component check, section 08). We did not test whether any flaw can be used here.

Evidence (section 08): E04 (OGC version check), E02 (OGC check), E03 (OGC capture).

WHAT TO DO

Remove the Windows policy that turns off Adobe's updater (bUpdater, found on this computer), then update Reader to the current version (Help, Check for Updates). If no one at the practice uses it, uninstall it instead.

ID OGC-DDS-F05 INSTALLED AS Adobe Acrobat Reader 23.006.20320 FLAWS SHOWN: 3 OF 155

CVE-2026-34621

CVE-2023-44336

CVE-2023-44337

NVD score: 8.8, as published

◆ FIX SOON

Outdated Software: Notepad++ 8.5.6

WAZUH AGENT

HIPAA Risk Management · 45 CFR 164.308(a)(1)(ii)(B)

What it is: This computer has Notepad++ 8.5.6 installed. Scanner data: Wazuh's feed matches 10 unique flaw IDs (CVEs) to this version by its version number, not reviewed one by one. Its highest-rated flaws score 7.8 out of 10.

Why it matters: Text and document editors open files that come from outside the practice. A crafted file can use a known editor flaw to run code when someone opens it.

Why Fix soon: A version match: the installed version falls in the range published flaws affect. The highest score Wazuh reports for its flaws is 7.8. A version match alone stays Fix soon until someone confirms a flaw can be reached on this computer. CVE-2025-15556 is on CISA's list, but it does not apply here: it lives in Notepad++'s automatic updater (GUP.exe). The installed program is C:\Program Files\Notepad++\notepad++.exe, and on 10-19-2026 we searched the whole C: drive: no GUP.exe and no updater folder anywhere. Windows' record of programs that have run has no entry for it either; that record can be incomplete, so it supports, but does not prove, that the updater never ran.

What we confirmed: The Wazuh agent read the version from the computer's list of installed software, and its server matched it against published flaw lists. We checked the CISA-listed flaw against the maker's advisory (table in section 08). We did not test whether any flaw can be used here.

Evidence (section 08): E01 (Wazuh agent), E02 (OGC check), E05 (OGC check).

WHAT TO DO

Download the current version directly from notepad-plus-plus.org and install it over the old one. Do not use the built-in updater of this old version. If no one at the practice uses it, uninstall it instead.

ID OGC-DDS-F03 INSTALLED AS Notepad++ (64-bit x64) 8.5.6 FLAWS SHOWN: 3 OF 10

CVE-2025-15556

CVE-2026-48778

CVE-2026-48800

Wazuh-reported score: 7.8, not recalculated

◆ FIX SOON

Outdated Software: VLC media player 3.0.11

WAZUH AGENT

HIPAA Risk Management · 45 CFR 164.308(a)(1)(ii)(B)

What it is: This computer has VLC media player 3.0.11 installed. Scanner data: Wazuh's feed matches 9 unique flaw IDs (CVEs) to this version by its version number, not reviewed one by one. The highest-rated, CVE-2023-47359, scores 9.8 out of 10.

Why it matters: A media player opens video and audio files from email, websites and USB drives. A crafted media file can use a known player flaw to run code on the computer.

Why Fix soon: A version match: the installed version falls in the range published flaws affect. The highest score Wazuh reports for its flaws is 9.8. A version match alone stays Fix soon until someone confirms a flaw can be reached on this computer.

What we confirmed: The Wazuh agent read the version from the computer's list of installed software, and its server matched it against published flaw lists. We did not test whether any flaw can be used here.

Evidence (section 08): E01 (Wazuh agent).

WHAT TO DO

Download the current version from videolan.org and install it over the old one. If no one at the practice uses it, uninstall it instead.

ID OGC-DDS-F04 INSTALLED AS VLC media player 3.0.11 FLAWS SHOWN: 3 OF 9

CVE-2023-47359

CVE-2023-46814

CVE-2022-41325

Wazuh-reported score: 9.8, not recalculated

— STRENGTHS

05 Strengths: none assessed

This check looked for weaknesses only, so we report no strengths. A fuller assessment would confirm settings such as the firewall, disk encryption and screen lock.

— FOR THE RECORD

06 Software inventory

Wazuh listed 30 installed programs on this computer (the full list is saved with the evidence), including the QEMU guest agent we leave out (see Excluded, section 08). Wazuh's feed matched flaws to four of them; our hand check added Adobe Reader, so five are in section 04. Wazuh's feed listed none for the rest, but it can miss a program, as it missed Adobe Reader. No network or port scan was run.

0 lower-priority items to review.

— ACTION PLAN

07 What to do, in order

One step per fix, most urgent first. The full instructions for each step are on its card in section 04.

01 Download the current version from 7-zip.org and install it over the old one. OGC-DDS-F01

Owner: Whoever looks after the practice's computers (the office manager, or your IT vendor if you have one).

Done when: the installed version is at or above the maker's fixed version for these flaws (or the program is uninstalled), recorded with the date, and the next Wazuh check agrees.

Recommended target: do within 1 week.

- 02** Remove the Windows policy that blocks Firefox updates (DisableAppUpdate, found on this computer), then update Firefox and check its automatic updates are on (Settings, General, Firefox Updates). OGC-DDS-F02

Owner: Whoever looks after the practice's computers (the office manager, or your IT vendor if you have one).

Done when: the installed version is at or above the maker's fixed version for these flaws (or the program is uninstalled), recorded with the date, and the next Wazuh check agrees.

Recommended target: do within 1 week.

- 03** Remove the Windows policy that turns off Adobe's updater (bUpdater, found on this computer), then update Reader to the current version (Help, Check for Updates). OGC-DDS-F05

Owner: Whoever looks after the practice's computers (the office manager, or your IT vendor if you have one).

Done when: the version in the program's About window is at or above the vendor's fixed version, and our recheck against the vendor's current bulletins finds no open flaw for it. Wazuh's feed missed this program, so the next Wazuh check alone is not proof.

Recommended target: do within 1 week.

- 04** Download the current version directly from notepad-plus-plus.org and install it over the old one. OGC-DDS-F03

Owner: Whoever looks after the practice's computers (the office manager, or your IT vendor if you have one).

Done when: the installed version is at or above the maker's fixed version for these flaws (or the program is uninstalled), recorded with the date, and the next Wazuh check agrees.

Recommended target: do within 30 days.

05

Download the current version from videolan.org and install it over the old one.

OGC-DDS-F04

Owner: Whoever looks after the practice's computers (the office manager, or your IT vendor if you have one).

Done when: the installed version is at or above the maker's fixed version for these flaws (or the program is uninstalled), recorded with the date, and the next Wazuh check agrees.

Recommended target: do within 2 weeks (published score 9.8, so sooner than the usual 30 days).

Status: nothing in this plan has been retested yet. To close an item, record against its ID which of these applies, the date, and the evidence:

- **Fixed:** the version now installed (from the program's About window or Windows' list of installed programs) is at or above the version the maker says fixes these flaws, recorded with the date. The next Wazuh check should agree, and the staff who use the program confirm it still works.
- **Not applicable:** a check shows that one specific flaw does not apply here, for example because the part of the program it lives in is not installed. Record what was checked and why. It closes that one flaw only.
- **Accepted risk:** you choose to keep the old version, for example because your dental software vendor requires it. Record the owner, the reason and what you do instead to reduce the risk.
- **Unresolved:** still open. Name the next step and the owner.

Recommended targets: Critical within 1 week, Fix soon within 30 days (2 weeks when its published score is 9.0 or higher). These are recommendations to plan around, not contract dates. If you cannot meet one, document the exception against the finding ID: the reason and a revised date.

METHOD

08 How this assessment was made

Tools

Wazuh agent 4.14.7 and Wazuh server 4.14.8: the agent lists the computer's installed software, and the server matches each program and version against published vulnerability lists; a hand check of a program Wazuh's feed missed, against the vendor's own bulletin and NVD; CISA's Known Exploited Vulnerabilities catalog dated 10-16-2026, with each listed flaw checked against the vendor's advisory.

When results were collected	10-19-2026, 7:20 PM: the software list and flaw matches were read from the Wazuh server. The hand checks were done the same day.
Scope	One front-desk computer running Windows 11 Pro, checked through the Wazuh agent installed on it. This computer is in One Guy Consulting's own test office and was set up with older versions of common office software. It is not a client's computer. Names are removed.
Device	One Microsoft Windows 11 Pro computer, version 10.0.26300.9457 (Wazuh agent 010).
Excluded	Every other computer and device at the practice was out of scope, as was the office network. We also left out one program, the QEMU guest agent: it exists only because this sample computer is a virtual machine, so a real front-desk computer would not have it. Wazuh listed 2 flaws for it.
Not tested	See Coverage below.
Saved records	Besides the files in the Evidence register: Wazuh's untouched answers for this computer (wazuh-raw-export.json, only the network address and computer name blanked), kept apart from our enriched copy (wazuh-host.json); and copies of every source we relied on (18 files: CISA's catalog, NVD records, and the Mozilla, 7-Zip and Adobe advisories), each with its address, download time and fingerprint (sources/SOURCES.json).
What we did not do	We did not try to break in, and no test traffic was sent to the computer. Its Wazuh agent reports the installed software to our Wazuh server.
Authorization	One Guy Consulting owns this test computer, so no outside permission was needed.
Evidence	Each finding points to a numbered entry in the Evidence register below: where the fact came from, when, and the saved file with its SHA-256 fingerprint (a code that changes if the file changes). We keep the saved files and give them to you on request.
Review	Not recorded. This is a draft and has not been reviewed for release.

Coverage

What we tested and what we did not. The findings apply only to what we tested.

TESTED	HOW
Installed software (Wazuh agent)	Software inventory and known vulnerabilities, read from inside the device.
Windows itself	Windows 11 Pro, version 10.0.26300.9457, checked the same way. Wazuh's feed listed no known flaws for it. We did not separately confirm its update level.
One program Wazuh's feed missed	Adobe Acrobat Reader, checked by hand against Adobe's bulletin APSB23-54, NVD and every Reader entry on CISA's list. Other installed programs were checked only through Wazuh's feed, which can miss a program, as it missed this one.
NOT TESTED	WHY
Other computers at the practice	Only the computer named in Scope was checked.
The office network and anything facing the internet	No network or port scan was run.
Device settings (firewall, disk encryption, screen lock, antivirus)	Not part of this report.
Whether any flaw can actually be used on this computer	We sent no attacks. Each finding is a version match.

CISA-listed flaws we checked

Each flaw on CISA's Known Exploited Vulnerabilities list that Wazuh or our hand check matched to an installed program, and how we decided whether it applies.

FLAW	PROGRAM (INSTALLED)	AFFECTED PART	FIXED IN	SOURCE	CONCLUSION
CVE-2025-0411	7-Zip (19.00)	archive extraction (download warning not passed on)	24.09	NVD CVE- 2025-0411 and 7-Zip history (24.09)	Applies
CVE-2026-34621	Adobe Acrobat Reader (23.006.20320)	PDF JavaScript (prototype pollution)	26.001.21411	Adobe APSB26- 43	Applies
CVE-2023-4863	Firefox (115.0)	WebP image decoding (libwebp, built into Firefox)	117.0.1	Mozilla MFSA 2023-40	Applies
CVE-2023-5217	Firefox (115.0)	VP8 video encoding (libvpx, built into Firefox)	118.0.1	Mozilla MFSA 2023-44	Applies
CVE-2024-9680	Firefox (115.0)	Animation timelines (browser engine)	131.0.2	Mozilla MFSA 2024-51	Applies
CVE-2025-15556	Notepad++ (8.5.6)	automatic updater (WinGUp)	8.8.9	NVD CVE- 2025- 15556 and our drive search	Not applicable: the updater is not on this computer

Evidence register

One entry per piece of evidence, numbered in the order the report cites it. Excerpts are shortened.

ID	ENTRY
E01 06C-DDS-F01, 06C-DDS-F02, 06C-DDS-F03, 06C-DDS-F04	Source: Wazuh server's software list and flaw matches for this computer Observed: 30 installed programs, including the QEMU guest agent we leave out; 4 with flaws in Wazuh's feed Wazuh agent, 10-19-2026, 7:20:05 PM EDT (UTC-4), captured at test time. 3-SCANS/wazuh-host.json SHA-256 3636072dec5a705eb16f60bd2c9946326c8a322e73f4af75375e16d0842fdb4d
E02 06C-DDS-F01, 06C-DDS-F02, 06C-DDS-F05, 06C-DDS-F03	Source: our check of each CISA-listed flaw against the vendor's advisory Observed: 6 CISA-listed flaws checked: 5 apply, CVE-2025-15556 does not. Each card names the advisory used. OGC check, 10-19-2026, 7:44:41 PM EDT (UTC-4), captured at test time. 3-SCANS/kev-validation.json SHA-256 011bd605679c87a0570b3d444923ceb3793840da6839d29e87d7c8cff9dcbb13
E03 06C-DDS-F01, 06C-DDS-F02, 06C-DDS-F05	Source: read-only check on the computer for the program's vulnerable part and update settings Observed: each flagged program's files and update settings, read from the computer (one record per program in the file) OGC capture, 10-19-2026, 7:53:14 PM EDT (UTC-4), captured at test time. 3-SCANS/component-check.txt SHA-256 ac1a1bde2da09a42b4a47e6e0a8828a552f05484b39af51420968145a2aa20a4
E04 06C-DDS-F05	Source: installed version compared by hand with the vendor's security bulletin Observed: Adobe Acrobat Reader 23.006.20320 installed; known flaws CVE-2026-34621, CVE-2023-44336, CVE-2023-44337, CVE-2023-44338 and more OGC version check, 10-19-2026, 7:31:18 PM EDT (UTC-4), captured at test time. 3-SCANS/version-check.json SHA-256 1dcfc6663c64d42b4b180872f6466808d736e37ced329d233f44c00dc8ae4284
E05 06C-DDS-F03	Source: search of the whole C: drive and Windows' record of programs that have run Observed: no GUP.exe and no updater folder anywhere on C:; no Prefetch entry for GUP.exe (Prefetch can be incomplete) OGC check, 10-19-2026, 7:44:41 PM EDT (UTC-4), captured at test time. 3-SCANS/notepadpp-updater-search.txt SHA-256 279d20c922f1af88fb8e8241f86fef88a1241e2dc6605ab7dbe737401409b25e

— IN CLOSING

Next steps and contact

WHAT HAPPENS NEXT

- Give each step in section 07 an owner and a date, most urgent first.
- When a fix is in place, ask us for a retest. We record the result against the finding ID.
- Send us any question about a finding or its fix.

REACH ONE GUY CONSULTING

- Email: hello@oneguyconsulting.com
- Phone: +1-646-694-8025
- Web: oneguyconsulting.com
- We store the raw scanner output for this engagement encrypted. How long we keep it is agreed for each engagement.

This report describes technical findings from an automated check of the computer named in scope. It is not legal advice. One Guy Consulting is not a law firm.

ABOUT THIS SAMPLE

This sample comes from a quick, automated check of one practice computer, so you can see the format. A full One Guy Consulting vulnerability scan goes further: every computer in scope, the office network, and everything your practice exposes to the internet.