keeliva Scanned November 10, 2026 · Network 10.0.10.x · harbourview.example · Confidential

Results from your scan

Grade



Needs Attention

Inside your network

One important problem to fix soon.

Priorities: 1 high, 4 medium, 3 low

Grade



Good

Visible from the internet

A few things worth tidying up. Nothing serious found.

Priorities: 1 medium, 1 low

Summary

✦ Written with AI from this report's findings

Inside your network, the most important item is that TIMESHEET-SRV (10.0.10.25) runs an older version of Apache HTTP Server, its web server software, with publicly known security problems; at least one of them is being used in attacks on other systems. Next in importance are remote desktop on PARTNER-PC (10.0.10.13), which any device on the network can reach, and the file storage device HV-FILES (10.0.10.20), which shares its folders with every device. Start with the actions below.

What to do first

1. **Have TIMESHEET-SRV (10.0.10.25) updated to a current Apache version, or ask your IT person whether it is still needed; then run the check again.**
   A device runs an older version of Apache HTTP Server with known security problems · Inside your network, finding 01
2. **Ask your IT person to limit remote desktop on PARTNER-PC (10.0.10.13) to the people who use it, or to switch it off if nobody does.**
   Devices can be remotely controlled over the network · Inside your network, finding 03
3. **Ask your IT person to restrict the shared folders on HV-FILES (10.0.10.20) to named users with passwords, instead of everyone on the network.**
   Your file storage device shares files with the whole network · Inside your network, finding 02

View this report online

Scan the code to open the report online.

Access code XXX-XXX

Your real report shows your private access code here.

https://keeliva.com/sample-report

Inside your network

What someone already connected to your network could see. We checked 13 devices. 1 has an important problem; 9 more have smaller items listed below.

Grade: Needs Attention

Network exposure	4 smaller findings	Good
Device hygiene	2 findings	Needs Attention
Network segmentation	1 smaller finding	Good
Wi-Fi security	Nothing found	Strong
Unknown devices	1 smaller finding	Good

Top findings

8 of 8, most important first

High priority · Likely affected

01

A device runs an older version of Apache HTTP Server with known security problems

Our AI review found strong signs that these known problems apply to this device. Your IT person can confirm.

In plain terms Apache HTTP Server 2.4.49 has publicly known problems that could let someone on your network read files on the server or make it stop responding. Updating the server's software closes them.

What we found
One device runs Apache HTTP Server version 2.4.49, which has publicly known security problems that attackers can use.

Why it matters
Someone who can reach the device over the network could use these known problems to get in, read data or stop the device from working. At least one of these problems is being used in attacks on other systems; that doesn't mean your network has been attacked.

What to do
Update the device's firmware or software to the latest version (ask your IT person or the device's vendor if you're not sure how), then run the check again. If no update is available, ask the vendor about a replacement, and meanwhile limit who can reach the device.

Where
Computer `TIMESHEET-SRV`

Details for your IT person: Technical details, item I1.

Medium priority

02

Your file storage device shares files with the whole network

What we found	A network storage device offers its files to every device on the network, including through older sharing methods.
Why it matters	If any share is open or uses a weak password, anyone on the network could read, change or encrypt (ransomware) all the files stored on it.
What to do	**Ask your IT person to check that every shared folder needs a password, to turn off sharing methods you don't use, and to keep an offline backup.**
Where	File server / network storage `HV-FILES (DS224+)`

Details for your IT person: Technical details, item I2.

Medium priority

03

Devices can be remotely controlled over the network

What we found	Remote screen control is switched on for one or more devices, so anyone who can reach them can try to log in.
Why it matters	If a password is weak or reused, an intruder could take over the device as if sitting at it; this is a common way ransomware gets in.
What to do	**Ask your IT person to confirm that remote control is really needed on these devices. If not, turn it off; if so, require strong passwords and limit who can connect.**
Where	Computer `PARTNER-PC`

Details for your IT person: Technical details, item I3.

Medium priority

04

Devices on your network could not be identified

What to do	**Check what each one is (look at device labels, ask staff). If nobody recognizes it, ask your IT person to look into it before taking any action.**
Where	Unknown device (vendor unknown)

Details for your IT person: Technical details, item I4.

SAMPLE

Medium priority

05

Smart and entertainment devices share the network with your computers

What to do

Ask your IT person to move smart/entertainment devices to a separate or guest network (many routers can do this), keeping your computers on their own network.

Details for your IT person: Technical details, item I5.

Low priority

06

Computers have file sharing switched on

What to do

Ask your IT person to confirm file sharing is meant to be on for these computers, that shared folders need a password, and that the oldest, least safe sharing method is turned off.

Where

- Computer `RECEPTION-PC`
- Computer `TAX-01`
- Computer `TAX-02`
- Computer `PARTNER-PC`
- Computer `TIMESHEET-SRV`

and 1 more (listed in the online report)

Details for your IT person: Technical details, item I6.

Low priority

07

Device settings pages are not encrypted

What to do

Ask your IT person to switch these settings pages to an encrypted connection if the device supports it, and to change any default admin passwords.

Where

- File server / network storage `HV-FILES (DS224+)`
- Printer `Brother MFC-L2750DW series`
- Phone system (VoIP) `SPA112`

Details for your IT person: Technical details, item I7.

SAMPLE

Low priority

08

A device on your network allows remote logins

What to do — **Ask your IT person to turn off remote logins on this device if they aren't needed, or make sure it uses a strong, non-default password.**

Where — File server / network storage `HV-FILES (DS224+)`

Details for your IT person: Technical details, item I8.

✓ 3 other devices: nothing found. They are listed in the online report.

Notes about this part

Couldn't verify

Our AI review thinks a known security problem in Apache HTTP Server 2.4.49 may not apply here, because it needs a feature or module there's no sign of. It isn't counted in the grade; ask your IT person to confirm.

Visible from the internet

What anyone on the internet can see about your network. We checked your internet address and harbourview.example.

Grade: Good

AI summary From the internet, the most important item is that fake email using your domain is not blocked: your domain's policy only asks other mail systems to report fakes, not to reject them. Something at your internet address also answers web requests; that is often the router's settings page, which your IT person should check. Your website certificate and your list of allowed email senders had no problems. Start with the actions below.

Services reachable from the internet	1 smaller finding	Strong
Email spoofing protection	1 smaller finding	Good
Website certificate & encryption	Nothing found	Strong

Top findings

2 of 2, most important first

Medium priority

01

Fake email using your domain is not blocked

What we found	Your domain's email policy is set to 'monitor only', so receiving mail servers are told to deliver fake email claiming to be from you anyway.
Why it matters	Fake emails using your exact address can still reach your clients' and staff's inboxes.
What to do	**Ask your IT person or email provider to change your domain's email policy from 'monitor only' to blocking fake email, once your real email passes the checks.**

Details for your IT person: Technical details, item E1.

Low priority

02

A web page is reachable at your internet address

What we found	Something on your network answers web requests from the internet. This may be intended (for example a VPN portal) or it may be your router's settings page.
Why it matters	If it's a settings or login page that isn't meant to be public, attackers can try guessed passwords or known flaws on it.
What to do	**Ask your IT person to check what this page is. If it's a router or device settings page, turn off access to it from the internet.**

Details for your IT person: Technical details, item E2.

Notes about this part

What the internet check covered

From our server we checked 10 commonly attacked services on your internet address. Not every possible service was checked, and nothing was tried beyond seeing whether each one answers.

SAMPLE

Technical details for your IT person

What we observed for each top finding. Addresses are on your network on the day of the scan. CVE numbers marked here are likely, not confirmed.

I1 A device runs an older version of Apache HTTP Server with known security problems

Service	`port 80 on 10.0.10.25 announces Apache HTTP Server 2.4.49` Device greeting: `Apache/2.4.49 (Unix)`
Known issue	`CVE-2021-42013; CVSS 9.8 (v3.1, rated by NVD); on CISA's known-exploited list; reason: Affects 2.4.49 and 2.4.50; the announced version is inside that range and nothing suggests a backported fix.`
Known issue	`CVE-2021-41773; CVSS 7.5 (v3.1, rated by NVD); on CISA's known-exploited list; reason: The announced version 2.4.49 is exactly the affected release, and the greeting shows no sign of a vendor or distribution patch.`
Known issue	`CVE-2021-41524; CVSS 7.5 (v3.1, rated by NVD); not on CISA's known-exploited list; reason: 2.4.49 is the only affected release and nothing in the greeting suggests a backported fix; the problem needs no special configuration.`

I2 Your file storage device shares files with the whole network

Exact steps	Ask your IT person to check that every share requires a password, to turn off sharing methods you don't use (such as NFS or old SMB versions), and to keep an offline backup.
Service	`port 139 (NetBIOS/SMB) open on 10.0.10.20`
Service	`port 445 (SMB) open on 10.0.10.20`

I3 Devices can be remotely controlled over the network

Exact steps	Ask your IT person to confirm remote desktop/screen sharing is needed on these devices; if not, turn it off; if so, require strong passwords, network-level login, and limit who can connect.
Service	`port 3389 (RDP) open on 10.0.10.13`

I4 Devices on your network could not be identified

Exact steps	Check what each one is (look at device labels, ask staff). If nobody recognizes it, ask your IT person to look into it before taking any action (the IP and hardware addresses help them find it).
Device	`maker not in the hardware-address registry; no self-reported name; open ports: none found`

SAMPLE

I5 Smart and entertainment devices share the network with your computers

Network	network 10.0.10.0/24: 8 computer/storage/printer device(s) and 1 consumer or smart-home device(s) (1 speaker / audio device) on the same network

I6 Computers have file sharing switched on

Exact steps	Ask your IT person to confirm file sharing is intended on these computers, that shared folders need a password, and that SMBv1 is turned off.
Service	port 139 (NetBIOS/SMB) open on 10.0.10.10
Service	port 445 (SMB) open on 10.0.10.10
Service	port 139 (NetBIOS/SMB) open on 10.0.10.11
Service	port 445 (SMB) open on 10.0.10.11
Service	port 139 (NetBIOS/SMB) open on 10.0.10.12
Service	port 445 (SMB) open on 10.0.10.12
Service	port 139 (NetBIOS/SMB) open on 10.0.10.13
Service	port 445 (SMB) open on 10.0.10.13
Service	port 139 (NetBIOS/SMB) open on 10.0.10.25
Service	port 445 (SMB) open on 10.0.10.25
Service	port 139 (NetBIOS/SMB) open on 10.0.10.50
Service	port 445 (SMB) open on 10.0.10.50

I7 Device settings pages are not encrypted

Exact steps	Ask your IT person to switch these settings pages to HTTPS if the device supports it, and to change any default admin passwords.
Service	port 80 (HTTP) open on 10.0.10.20; no encrypted (HTTPS) alternative was found Device greeting: `HTTP/1.1 200 OK | Server: nginx`
Service	port 80 (HTTP) open on 10.0.10.30; no encrypted (HTTPS) alternative was found Device greeting: `HTTP/1.1 200 OK | Server: debut/1.30`
Service	port 80 (HTTP) open on 10.0.10.91; no encrypted (HTTPS) alternative was found Device greeting: `HTTP/1.1 200 OK | Server: mini_httpd`

SAMPLE

I8 A device on your network allows remote logins

Exact steps	Ask your IT person to turn off remote login (SSH) on this device if it isn't needed, or make sure it uses a strong, non-default password.
Service	`port 22 (SSH) open on 10.0.10.20` Device greeting: `SSH-2.0-OpenSSH_8.2p1`

E1 Fake email using your domain is not blocked

Exact steps	Ask your IT person or email provider to move the DMARC policy from p=none to p=quarantine, then p=reject, once your real email passes the checks.
Email record	`DMARC for harbourview.example: policy is p=none (monitoring only); record: v=DMARC1; p=none; rua=mailto:dmarc@harbourview.example`

E2 A web page is reachable at your internet address

Exact steps	Ask your IT person to check what this page is. If it's a router or device settings page, turn off remote (WAN-side) management.
Service	`port 443 (HTTPS web) answered from the internet on 203.0.113.42`

View this report online

The online report has the same findings. Anyone you share the link and code with can view it.

Link

`https://keeliva.com/sample-report`

Access code

XXX-XXX

Your real report shows your private access code here.

A real report's link and code work for 90 days after the scan, or while a monthly plan is active. The QR code opens the link only; the access code is never in it.

About this scan

What this scan did

- Looked for devices on your network from one computer
- Checked 35 common services on each device, gently and one step at a time
- Read the short greeting some devices send, to see what software they run
- Compared software versions with public lists of known security problems

What it didn't do

- Try any passwords or log in to anything
- Change any settings or install anything on your devices
- Read your files, emails or browsing
- Send your Wi-Fi name or passwords anywhere

When

November 10, 2026, about 1 minute. Safe for business hours.

How to read the grades

Each part is graded by its most important finding, so one serious problem is never hidden by many clean areas. Our AI writes the plain-language explanations and double-checks possible software problems, and may set aside ones that don't apply. Grades and priorities come from fixed rules.

Fixed something? Scan again to confirm Open Keeliva on the computer you scanned from and run the scan again: your new grade and problem counts show right away, free. To see the updated full report, with every finding re-checked, choose the monthly plan (re-scans included: first month US$19.99, then US$7.99 a month; your report stays online with no 90-day limit; cancel any time, you keep access until the end of the month you've paid for) or buy a single new report at US$19.99.

`Text in this style` was reported by devices on your network and is shown exactly as received.

SAMPLE