Plain-English Security Review

Tenant: **C-[sample]**
Week of: **2026-05-25**
Source report: **scan-154**
Scan completed: **05/25/2026, 04:00 PM EDT**
Generated: **05/25/2026, 04:00 PM EDT**
Time zone: **US Eastern (ET)**

Security Summary

We found 37 security issues across 5 devices. 5 need urgent attention. 16 should be fixed soon. Start with Server2, 192.168.1.90, and GS308EP.

A network doorway is a way into a device or service. Some doorways are normal and needed. This report points out doorways IT should review.

Good News

- The scan completed with enough information to prioritize the first fixes.

What Needs Attention

Urgent issues — 5
Needs quick attention.

Important issues — 16
Should be fixed soon.

Planned issues — 1
Schedule into normal IT work.

Routine issues — 15
Review when time allows.

What To Do Next

1. **Review the devices that need attention first.**
   Owner: IT Lead **Due date:** Next business day
   How to confirm: Confirm each issue has an owner.

2. **Fix urgent and important security issues.**
   Owner: IT Ops **Due date:** As scheduled by IT
   How to confirm: Run a follow-up scan.

3. **Confirm reachable services are expected.**
   Owner: IT Ops **Due date:** Within 7 days
   How to confirm: Confirm each service is needed and protected.

Report Coverage

This section shows how much information was available. If a device was not visible during the scan, the report may not show its current security state.

SECURITY SCAN COVERAGE	5 devices with reportable issues
SECURITY ISSUES FOUND	37
DATA NOT COLLECTED	Devices outside the configured scan target, offline devices, blocked devices, or devices not visible from the scan source may not appear here.

5	37	5	16
DEVICES	TOTAL ISSUES	URGENT	IMPORTANT

Top Risks First

Start here before reading the full issue list.

Urgent Slow connection protection

DEVICE

Server1, 192.168.1.240

RECOMMENDED ACTION

Ask IT to limit slow or excessive connections and test again.

Urgent Older web security settings

DEVICE

Server1, 192.168.1.240

RECOMMENDED ACTION

Ask IT to update the web security settings and test again.

Urgent Slow connection protection

DEVICE

Server1, 192.168.1.240

RECOMMENDED ACTION

Ask IT to limit slow or excessive connections and test again.

Urgent Slow connection protection

DEVICE

Server2, 192.168.1.90

RECOMMENDED ACTION

Ask IT to limit slow or excessive connections and test again.

Urgent Private website files visible

DEVICE

Server3, 192.168.1.158

RECOMMENDED ACTION

Ask IT to block access to private website files.

Important Outdated software

DEVICE

Server1, 192.168.1.240

RECOMMENDED ACTION

Treat this as urgent. Patch as soon as possible, limit exposure if patching must wait, and monitor the affected systems closely until fixed. Handle it in the current fix window.

Security Issues and Next Steps

This section translates each issue found into plain language and gives a practical next step. Technical scanner output is provided later for IT.

Server1

dev.blackframerp.net • 192.168.1.240

Urgent

Urgent **Slow connection protection**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
The site may become slow or unavailable for users.

NEXT STEP
Ask IT to limit slow or excessive connections and test again.

Urgent **Older web security settings**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
Private information may not be protected as strongly as it should be.

NEXT STEP
Ask IT to update the web security settings and test again.

Urgent **Slow connection protection**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
The site may become slow or unavailable for users.

NEXT STEP
Ask IT to limit slow or excessive connections and test again.

Important

Important **Outdated software**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Treat this as urgent. Patch as soon as possible, limit exposure if patching must wait, and monitor the affected systems closely until fixed. Handle it in the current fix window.

Important **Outdated software**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Treat this as urgent. Patch as soon as possible, limit exposure if patching must wait, and monitor the affected systems closely until fixed. Handle it in the current fix window.

Important **Reachable service review**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
Risk: An important service is open and can be accessed from the internet. This could allow unwanted visitors to reach your system. Business impact: If this issue is not fixed, it may lead to unauthorized access or problems with your services.

NEXT STEP
Update the software or change its settings to make it safer. After making changes, check again to ensure the problem is resolved.

Important **Reachable service review**

DEVICE
Server1, 192.168.1.240

AREA
Web service

WHY IT MATTERS
Risk: An exposed service on network doorway 80 can allow unwanted access to your system. This is a serious issue that needs to be fixed quickly. Business impact: If not addressed, this could lead to unauthorized access or problems with your services.

NEXT STEP
Update the software or change the settings for the affected service. After making changes, check again to ensure the issue is resolved.

Routine

Routine **Reachable service review**

DEVICE
Server1, 192.168.1.240

AREA
File sharing service

WHY IT MATTERS
Risk: There is a service running that could be seen by others on the internet. This may allow unwanted access to your system. Business impact: If not addressed, this issue could lead to security problems or disruptions in your operations over time.

NEXT STEP
Update the software or change the settings for this service to make it safer. After making changes, check again to ensure the issue is fixed.

Routine **Reachable service review**

DEVICE
Server1, 192.168.1.240

AREA
File sharing service

WHY IT MATTERS
Risk: An exposed service on network doorway 139/tcp may allow unauthorized access to your system. This could lead to potential security issues if not addressed. Business impact: If this issue is not fixed, it could increase the risk of security problems or operational disruptions...

NEXT STEP
To reduce risk, update the affected service or change its settings as recommended by the vendor. After making changes, check again to ensure the issue is resolved.

Routine **Reachable service review**

DEVICE
Server1, 192.168.1.240

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 135 that could be seen by others. This might allow unwanted access to your system. Business impact: If this issue is not fixed, it could lead to more problems with security or operations in the future.

NEXT STEP
Update the software or change the settings for this service to make it safer. After that, check again to ensure the issue is resolved.

Server2

192.168.1.90

Urgent

Urgent **Slow connection protection**

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
The site may become slow or unavailable for users.

NEXT STEP
Ask IT to limit slow or excessive connections and test again.

Important

Important **Outdated software**

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Update the affected software to a safer supported version and retire anything too old to patch.

Important **Outdated software**

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Update the affected software to a safer supported version and retire anything too old to patch.

Important **Information exposure**

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Private or sensitive data may be exposed.

NEXT STEP
Patch the affected service and double-check that sensitive data paths are properly restricted.

Important **Security issue found**

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
It adds avoidable risk to the system.

NEXT STEP
Assign someone to fix it, make the change, and confirm it no longer appears on a follow-up scan.

Important **Outdated software**

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Update the affected software to a safer supported version and retire anything too old to patch.

Routine

Routine **Reachable service review**

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 9100 that is visible to the internet. This could allow unwanted access, which is a security concern. Business impact: If this issue is not fixed, it may lead to increased risks for your operations and security over time.

NEXT STEP
It is advised to update the service or change its settings to make it more secure. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Risk: There is a service running on network doorway 8080 that could be accessed by anyone on the internet. This may lead to security issues if not addressed. Business impact: If this issue is not fixed, it could lead to increased risks for your operations and security over time.

NEXT STEP
Update the software or change its settings to make it more secure. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 631 that could be seen by outsiders. This may create a small security risk that should be monitored. Business impact: If this issue is not fixed, it could lead to bigger security problems or affect how the business operates over...

NEXT STEP
It's best to update the software or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a printer service that is open to the internet, which could allow unauthorized access. This is considered a low-level security risk. Business impact: If this issue is not fixed, it may lead to bigger security problems or operational issues in the future.

NEXT STEP
Update the printer's software or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Risk: There is a service running on network doorway 443 that is exposed to the internet. This means it could be accessed by anyone, which may lead to security issues over time. Business impact: If this issue is not fixed, it could lead to increased risks for your operations and s...

NEXT STEP
It's important to update the service or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 81 that is visible to the internet. This could allow unwanted access or attacks if not managed properly. Business impact: If this issue is not fixed, it may lead to increased risks for your operations and security over time.

NEXT STEP
Update the service or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Web service

WHY IT MATTERS
Risk: There is a service running on a common internet network doorway (80) that could be seen by others. This means there is a small chance of security issues if not managed properly. Business impact: If this issue is not fixed, it could lead to bigger security problems or affect...

NEXT STEP
It is advised to update the software or change its settings to make it more secure. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 23 that could be seen by others. This means it might be easier for someone to access your system without permission. Business impact: If this issue is not fixed, it could lead to problems with your operations or security over ti...

NEXT STEP
It's best to update the software or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE
Server2, 192.168.1.90

AREA
Reachable service

WHY IT MATTERS
Risk: There is a service running on network doorway 21 that is visible to the internet. This could allow unauthorized access if not managed properly. Business impact: If this issue is not fixed, it may lead to security problems or operational disruptions in the future.

NEXT STEP
Update the software or change the settings for the service on network doorway 21. After making changes, check again to ensure the issue is resolved.

Server3

192.168.1.158

Urgent

Urgent Private website files visible

DEVICE
Server3, 192.168.1.158

AREA
Web service

WHY IT MATTERS
Someone could learn details that make the system easier to attack.

NEXT STEP
Ask IT to block access to private website files.

Important

Important File access control issue

DEVICE
Server3, 192.168.1.158

AREA
Web service

WHY IT MATTERS
Private files, settings, or secrets may be easier to reach.

NEXT STEP
Fix the file-path handling and block requests that try to reach folders outside the allowed area.

Important File access control issue

DEVICE
Server3, 192.168.1.158

AREA
Web service

WHY IT MATTERS
Private files, settings, or secrets may be easier to reach.

NEXT STEP
Fix the file-path handling and block requests that try to reach folders outside the allowed area.

Important Missing access check

DEVICE
Server3, 192.168.1.158

AREA
Web service

WHY IT MATTERS
Someone may be able to reach a sensitive function without proper approval.

NEXT STEP
Require sign-in and permission checks anywhere this feature can be reached.

Important **Reachable service review**

DEVICE
Server3, 192.168.1.158

AREA
Web service

WHY IT MATTERS
Risk: An open service on network doorway 80 can allow unwanted access to your system. This is a serious issue that needs quick attention. Business impact: If not fixed, this could lead to unauthorized access or problems with your services.

NEXT STEP
Update the service or change its settings to make it safer. After making changes, check again to ensure the issue is resolved.

Server4

192.168.1.100

Important

Important **Security issue found**

DEVICE
Server4, 192.168.1.100

AREA
Web service

WHY IT MATTERS
It adds avoidable risk to the system.

NEXT STEP
Assign someone to fix it, make the change, and confirm it no longer appears on a follow-up scan.

Important **Outdated software**

DEVICE
Server4, 192.168.1.100

AREA
Remote access service

WHY IT MATTERS
Known bugs in old software are easier for attackers to target.

NEXT STEP
Update the affected software to a safer supported version and retire anything too old to patch.

Important **Reachable service review**

DEVICE
Server4, 192.168.1.100

AREA
Web service

WHY IT MATTERS
Risk: There is a service running on a public network doorway that could be accessed by anyone. This increases the chance of unauthorized access or problems with the service. Business impact: If this issue is not fixed, it could lead to security breaches or disruptions in service.

NEXT STEP
Update the software or change the settings of the affected service to make it safer. After making changes, check again to ensure the issue is resolved.

Planned

Planned

Reachable service review

DEVICE
Server4, 192.168.1.100

AREA
Remote access service

WHY IT MATTERS
Risk: There is a service running on network doorway 22 that could be accessed by unauthorized users. This may lead to security issues if not addressed. Business impact: If this issue is not fixed, it could lead to increased risks for the organization over time.

NEXT STEP
Update the software or change its settings to make it more secure. After making changes, check again to ensure the problem is resolved.

Server5

192.168.1.165

Routine

Routine

Reachable service review

DEVICE
Server5, 192.168.1.165

AREA
File sharing service

WHY IT MATTERS
Risk: There is a service running that could be seen by others on the internet. This may allow unwanted access to your system. Business impact: If not addressed, this issue could lead to security problems or disruptions in your operations over time.

NEXT STEP
Update the software or change the settings for this service to make it safer. After making changes, check again to ensure the issue is fixed.

Routine

Reachable service review

DEVICE
Server5, 192.168.1.165

AREA
File sharing service

WHY IT MATTERS
Risk: An exposed service on network doorway 139/tcp may allow unauthorized access to your system. This could lead to potential security issues if not addressed. Business impact: If this issue is not fixed, it could increase the risk of security problems or operational disruptions...

NEXT STEP
To reduce risk, update the affected service or change its settings as recommended by the vendor. After making changes, check again to ensure the issue is resolved.

Routine

Reachable service review

DEVICE

Server5, 192.168.1.165

AREA

Reachable service

WHY IT MATTERS

Risk: There is a service running on network doorway 135 that could be seen by others. This might allow unwanted access to your system. Business impact: If this issue is not fixed, it could lead to more problems with security or operations in the future.

NEXT STEP

Update the software or change the settings for this service to make it safer. After that, check again to ensure the issue is resolved.

Report Notes

This weekly security visibility report is informational only and is not a formal audit, certification, compliance report, penetration test, insurance outcome guarantee, or breach-prevention guarantee. It is intended to support visibility and planning for network and device security work.

Results are based on point-in-time scan visibility and configured scope. Devices that are offline, segmented, blocked by controls, not credentialed, or otherwise out of scope may not be represented. No scan report can guarantee identification of every security issue.

Use this report for priority planning: address urgent and important issues first, validate major changes before disrupting production, and track fixes over time with follow-up scans. Final fix and acceptance decisions remain with your organization's leadership and IT/security owners.

This report can help show that security is being actively managed, but insurance outcomes are not guaranteed. Contact your insurance representative for policy-specific details.

Questions about this report can be submitted through the support page at https://portal.shawtechpgh.com/support. Technical fix and implementation questions should be directed to your internal or contracted IT team.

Technical terms: Official security issue ID means CVE. Technical severity score means CVSS. Exact network doorway numbers, scanner plugin names, and raw evidence are preserved below for IT.

Technical Details for IT

You do not need to read this section unless you manage the system or are creating a repair ticket.

This section preserves CVE IDs, CVSS scores, exact ports/protocols, scanner plugin names, and raw evidence for validation, engineering review, and ticket documentation.

Server1

dev.blackframerp.net • 192.168.1.240

THREAT	CVSS	PORT	FINDING
critical	9.3	443/tcp	**Scan Discovery: http-slowloris-check** **CVE:** CVE-2007-6750 VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE:CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 http://ha.ckers.org/slowloris/
critical	9.3	443/tcp	**Scan Discovery: ssl-dh-params** VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength State: VULNERABLE Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks. Check results: WEAK DH GROUP 1 Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 Modulus Type: Safe prime Modulus Source: RFC2409/Oakley Group 2 Modulus Length: 1024 Generator Length: 8 Public Key Length: 1024 [Evidence output truncated for readability]
critical	9.3	80/tcp	**Scan Discovery: http-slowloris-check**

THREAT	CVSS	PORT	FINDING
			CVE: CVE-2007-6750 VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE:CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 http://ha.ckers.org/slowloris/
high	8.1	443/tcp	**Scan Discovery: vulners** **CVE:** CVE-2026-28780 CVE-2024-38476 CVE-2024-38474 CVE-2025-23048 CVE-2024-40898 CVE-2024-38475 cpe:/a:apache:http_server:2.4.58: CVE-2026-28780 9.8 https://vulners.com/cve/CVE-2026-28780 CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476 CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474 CNVD-2024-36391 9.8 https://vulners.com/cnvd/CNVD-2024-36391 CNVD-2024-36388 9.8 https://vulners.com/cnvd/CNVD-2024-36388 PACKETSTORM:213257 9.1 https://vulners.com/packetstorm/PACKETSTORM:213257 *EXPLOIT* FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1 https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F *EXPLOIT* FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 9.1 https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 *EXPLOIT* E606D7F4-5FA2-5907-B30E-367D6FFECD89 9.1 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89 *EXPLOIT* D8A19443-2A37-5592-8955-F614504AAF45 9.1 https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45 *EXPLOIT* CVE-2025-23048 9.1 https://vulners.com/cve/CVE-2025-23048 CVE-2024-40898 9.1 https://vulners.com/cve/CVE-2024-40898 CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475 [Evidence output truncated for readability]
high	8.1	80/tcp	**Scan Discovery: vulners**

THREAT	CVSS	PORT	FINDING
			CVE: CVE-2026-28780 CVE-2024-38476 CVE-2024-38474 CVE-2025-23048 CVE-2024-40898 CVE-2024-38475 cpe:/a:apache:http_server:2.4.58: CVE-2026-28780 9.8 https://vulners.com/cve/CVE-2026-28780 CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476 CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474 CNVD-2024-36391 9.8 https://vulners.com/cnvd/CNVD-2024-36391 CNVD-2024-36388 9.8 https://vulners.com/cnvd/CNVD-2024-36388 PACKETSTORM:213257 9.1 https://vulners.com/packetstorm/PACKETSTORM:213257 *EXPLOIT* FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1 https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F *EXPLOIT* FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 9.1 https://vulners.com/githubexploit/FBC8A8BE-F00A-5B6D-832E-F99A72E7A3F7 *EXPLOIT* E606D7F4-5FA2-5907-B30E-367D6FFECD89 9.1 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89 *EXPLOIT* D8A19443-2A37-5592-8955-F614504AAF45 9.1 https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45 *EXPLOIT* CVE-2025-23048 9.1 https://vulners.com/cve/CVE-2025-23048 CVE-2024-40898 9.1 https://vulners.com/cve/CVE-2024-40898 CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475 [Evidence output truncated for readability]
high	7.5	443/tcp	**Exposed service on 443/tcp** Detected http Apache httpd 2.4.58
high	7.5	80/tcp	**Exposed service on 80/tcp** Detected http Apache httpd 2.4.58
low	3.1	445/tcp	**Exposed service on 445/tcp** Detected microsoft-ds
low	3.1	139/tcp	**Exposed service on 139/tcp** Detected netbios-ssn Microsoft Windows netbios-ssn
low	3.1	135/tcp	**Exposed service on 135/tcp** Detected msrpc Microsoft Windows RPC

Server2

192.168.1.90

THREAT	CVSS	PORT	FINDING
critical	9.3	631/tcp	**Scan Discovery: http-slowloris-check** **CVE:** CVE-2007-6750 VULNERABLE: Slowloris DOS attack State: LIKELY VULNERABLE IDs: CVE:CVE-2007-6750 Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service. Disclosure date: 2009-09-17 References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750 http://ha.ckers.org/slowloris/
high	8.1	8080/tcp	**Scan Discovery: vulners** **CVE:** CVE-2021-21783 CVE-2020-13576 CVE-2019-7659 CVE-2017-9765 CVE-2024-4227 CVE-2020-13578 CVE-2020-13577 CVE-2020-13575 CVE-2020-13574 cpe:/a:genivia:gsoap:2.7: CVE-2021-21783 9.8 https://vulners.com/cve/CVE-2021-21783 CVE-2020-13576 9.8 https://vulners.com/cve/CVE-2020-13576 CVE-2019-7659 8.1 https://vulners.com/cve/CVE-2019-7659 CVE-2017-9765 8.1 https://vulners.com/cve/CVE-2017-9765 CNVD-2017-15493 8.1 https://vulners.com/cnvd/CNVD-2017-15493 CVE-2024-4227 7.5 https://vulners.com/cve/CVE-2024-4227 CVE-2020-13578 7.5 https://vulners.com/cve/CVE-2020-13578 CVE-2020-13577 7.5 https://vulners.com/cve/CVE-2020-13577 CVE-2020-13575 7.5 https://vulners.com/cve/CVE-2020-13575 CVE-2020-13574 7.5 https://vulners.com/cve/CVE-2020-13574 SSV:96284 6.8 https://vulners.com/seebug/SSV:96284 *EXPLOIT*
high	8.1	631/tcp	**Scan Discovery: vulners** **CVE:** CVE-2021-21783 CVE-2020-13576 CVE-2019-7659 CVE-2017-9765 CVE-2024-4227 CVE-2020-13578 CVE-2020-13577 CVE-2020-13575 CVE-2020-13574 cpe:/a:genivia:gsoap:2.7: CVE-2021-21783 9.8 https://vulners.com/cve/CVE-2021-21783 CVE-2020-13576 9.8 https://vulners.com/cve/CVE-2020-13576 CVE-2019-7659 8.1 https://vulners.com/cve/CVE-2019-7659 CVE-2017-9765 8.1 https://vulners.com/cve/CVE-2017-9765 CNVD-2017-15493 8.1 https://vulners.com/cnvd/CNVD-2017-15493

THREAT	CVSS	PORT	FINDING
			CVE-2024-4227 7.5 https://vulners.com/cve/CVE-2024-4227 CVE-2020-13578 7.5 https://vulners.com/cve/CVE-2020-13578 CVE-2020-13577 7.5 https://vulners.com/cve/CVE-2020-13577 CVE-2020-13575 7.5 https://vulners.com/cve/CVE-2020-13575 CVE-2020-13574 7.5 https://vulners.com/cve/CVE-2020-13574 SSV:96284 6.8 https://vulners.com/seebug/SSV:96284 *EXPLOIT*
high	8.1	443/tcp	**Scan Discovery: ssl-ccs-injection** **CVE:** CVE-2014-0224 VULNERABLE: SSL/TLS MITM vulnerability (CCS Injection) State: VULNERABLE Risk factor: High OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability. References: http://www.cvedetails.com/cve/2014-0224 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 http://www.openssl.org/news/secadv_20140605.txt
high	8.1	443/tcp	**Scan Discovery: ssl-poodle** **CVE:** CVE-2014-3566 VULNERABLE: SSL POODLE information leak State: VULNERABLE IDs: BID:70574 CVE:CVE-2014-3566 The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue. Disclosure date: 2014-10-14 Check results: TLS_RSA_WITH_AES_128_CBC_SHA References: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 https://www.imperialviolet.org/2014/10/14/poodle.html [Evidence output truncated for readability]
high	8.1	80/tcp	**Scan Discovery: vulners** **CVE:** CVE-2021-21783 CVE-2020-13576 CVE-2019-7659 CVE-2017-9765 CVE-2024-4227 CVE-2020-13578 CVE-2020-13577 CVE-2020-13575 CVE-2020-13574

THREAT	CVSS	PORT	FINDING
			cpe:/a:genivia:gsoap:2.7: CVE-2021-21783 9.8 https://vulners.com/cve/CVE-2021-21783 CVE-2020-13576 9.8 https://vulners.com/cve/CVE-2020-13576 CVE-2019-7659 8.1 https://vulners.com/cve/CVE-2019-7659 CVE-2017-9765 8.1 https://vulners.com/cve/CVE-2017-9765 CNVD-2017-15493 8.1 https://vulners.com/cnvd/CNVD-2017-15493 CVE-2024-4227 7.5 https://vulners.com/cve/CVE-2024-4227 CVE-2020-13578 7.5 https://vulners.com/cve/CVE-2020-13578 CVE-2020-13577 7.5 https://vulners.com/cve/CVE-2020-13577 CVE-2020-13575 7.5 https://vulners.com/cve/CVE-2020-13575 CVE-2020-13574 7.5 https://vulners.com/cve/CVE-2020-13574 SSV:96284 6.8 https://vulners.com/seebug/SSV:96284 *EXPLOIT*
low	3.1	9100/tcp	**Exposed service on 9100/tcp** Detected jetdirect
low	3.1	8080/tcp	**Exposed service on 8080/tcp** Detected soap gSOAP 2.7
low	3.1	631/tcp	**Exposed service on 631/tcp** Detected soap gSOAP 2.7
low	3.1	515/tcp	**Exposed service on 515/tcp** Detected printer
low	3.1	443/tcp	**Exposed service on 443/tcp** Detected tcpwrapped
low	3.1	81/tcp	**Exposed service on 81/tcp** Detected tcpwrapped
low	3.1	80/tcp	**Exposed service on 80/tcp** Detected soap gSOAP 2.7
low	3.1	23/tcp	**Exposed service on 23/tcp** Detected telnet Pocket CMD telnetd
low	3.1	21/tcp	**Exposed service on 21/tcp** Detected ftp oftpd

Server3

192.168.1.158

THREAT	CVSS	PORT	FINDING
critical	9.3	80/tcp	**Scan Discovery: http-litespeed-sourcecode-download** **CVE:** CVE-2010-2333 Litespeed Web Server Source Code Disclosure (CVE-2010-2333) /index.php source code: Redirect to Login top.location.href = "/login.cgi";
high	8.1	80/tcp	**Scan Discovery: http-phpmyadmin-dir-traversal** **CVE:** CVE-2005-3299 VULNERABLE: phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion State: UNKNOWN (unable to test) IDs: CVE:CVE-2005-3299 PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array. Disclosure date: 2005-10-nil Extra information: ../../../../../etc/passwd : Redirect to Login top.location.href = "/login.cgi"; [Evidence output truncated for readability]
high	8.1	80/tcp	**Scan Discovery: http-enum** **CVE:** CVE-2009-3733 /sdk/../../../../../../../etc/vmware/hostd/vmInventory.xml: Possible path traversal in VMWare (CVE-2009-3733) /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml: Possible path traversal in VMWare (CVE-2009-3733) /../../../../../../../../../../etc/passwd: Possible path traversal in URI /../../../../../../../../../../boot.ini: Possible path traversal in URI
high	8.1	80/tcp	**Scan Discovery: http-vuln-cve2010-0738** /jmx-console/: Authentication was not required
high	7.5	80/tcp	**Exposed service on 80/tcp** Detected http

Server4

192.168.1.100

THREAT	CVSS	PORT	FINDING
high	8.1	443/tcp	**Scan Discovery: http-vuln-cve2011-3192** **CVE:** CVE-2011-3192 VULNERABLE: Apache byterange filter DoS State: VULNERABLE IDs: BID:49303 CVE:CVE-2011-3192 The Apache web server is vulnerable to a denial of service attack when numerous overlapping byte ranges are requested. Disclosure date: 2011-08-19 References: https://seclists.org/fulldisclosure/2011/Aug/175 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192 https://www.tenable.com/plugins/nessus/55976 https://www.securityfocus.com/bid/49303
high	8.1	22/tcp	**Scan Discovery: vulners** **CVE:** CVE-2023-38408 CVE-2023-28531 cpe:/a:openbsd:openssh:8.9p1: PACKETSTORM:179290 10.0 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT* 1EEC8894-D2F7-547C-827C-915BE866875C 10.0 https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-915BE866875C *EXPLOIT* 09B905C6-CD97-54E6-AD97-B0DD1AC4771B 10.0 https://vulners.com/githubexploit/09B905C6-CD97-54E6-AD97-B0DD1AC4771B *EXPLOIT* PACKETSTORM:173661 9.8 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT* F0979183-AE88-53B4-86CF-3AF0523F3807 9.8 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT* CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408 CVE-2023-28531 9.8 https://vulners.com/cve/CVE-2023-28531 B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT* A2B36B85-C737-548F-8C04-9339EDCDBFF5 9.8 https://vulners.com/githubexploit/A2B36B85-C737-548F-8C04-9339EDCDBFF5 *EXPLOIT* 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT* 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8

THREAT	CVSS	PORT	FINDING
			https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT* 6192C35D-F78B-5C0A-AB8D-9826A79A5320 9.8 https://vulners.com/githubexploit/6192C35D-F78B-5C0A-AB8D-9826A79A5320 *EXPLOIT* 33D623F7-98E0-5F75-80FA-81AA666D1340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EXPLOIT* [Evidence output truncated for readability]
high	7.5	443/tcp	**Exposed service on 443/tcp** Detected http nginx
medium	5.3	22/tcp	**Exposed service on 22/tcp** Detected ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.15

Server5

192.168.1.165

THREAT	CVSS	PORT	FINDING
low	3.1	445/tcp	**Exposed service on 445/tcp** Detected microsoft-ds
low	3.1	139/tcp	**Exposed service on 139/tcp** Detected netbios-ssn Microsoft Windows netbios-ssn
low	3.1	135/tcp	**Exposed service on 135/tcp** Detected msrpc Microsoft Windows RPC