Your response plan

Prepared from your answers. Bring the evidence, agree the next move, leave with an owner.

Team	Example team (illustrative)
System / service	Customer portal (illustrative)
Accountable owner	Service owner (example)
Next review	2026-11-09

Turn the open questions into owned actions.

Agree the next decision, an accountable person and the evidence needed to close the work. Use your security team's judgement to set the deadline.

What is established?

8 of 8 questions answered beyond "unknown". This is not a security score.

Affected systems	Yes, a match is confirmed
Access	Yes, it is internet-facing
Business impact	Essential operations or sensitive data
Suspicious activity	No signs reported after checking
Accountability	Yes, an owner is agreed
Progress	Installed, but not yet verified
Change safety	Yes, the plan is recorded
Evidence	No, evidence is missing

The action register

Use this as your meeting agenda. Agree actual owners and deadlines; suggested checkpoints below are not security SLAs.

Advisory / ticket	Add the actual vendor advisory and internal ticket
Possible blocker	Confirm the running version after the restart and check the customer login flow.

01 Agree the urgency with your security team

Consider reachable systems, business impact and evidence of exploitation. Check the vendor advisory and CISA's known-exploited list; use these as inputs, not an automatic score.

Suggested owner: Security lead + business owner

Assigned to: Unassigned - agree owner | Due: Agree with owner

Checkpoint: Before agreeing a change deadline

Bring back: Priority rationale, affected services and approved target date

02 Verify the running system, not just the ticket

Confirm the running version or configuration, repeat the relevant check and verify that the service works. Record unresolved items with an owner and review date.

Suggested owner: Technical verifier + accountable owner

Assigned to: Unassigned - agree owner | Due: Agree with owner

Checkpoint: After deployment, before closure

Bring back: Running-state evidence, check result, service-health result and exception record

Make the handoff count.

A 15-minute conversation that ends with a decision, a person and a next review.

First 5 minutes

Establish the facts

Which advisory applies? Which systems were checked? What is confirmed, and what is still an assumption?

Next 5 minutes

Agree the response

What is the next action, who owns it and what deadline is justified? What approval, access or supplier response is blocking it?

Final 5 minutes

Define “done”

What evidence will confirm the running system is fixed and the service still works? Who accepts any unresolved exception, and when is it reviewed?

Do not close on “the ticket is done”.

- ☐ Running product version or configuration recorded
- ☐ Relevant check repeated after the change
- ☐ Business service confirmed healthy
- ☐ Exceptions named, owned and given a review date

Decision / agreed next action

Owner / due date / evidence location