Network Capture Troubleshooting Report

tcp_zerowindowdead.pcapng

Report ID	PCAI-2026-1106-8HSK
Version	1 (Sample)
Generated	2026-11-06 11:18:51 UTC
Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Classification	TLP:CLEAR

SAMPLE

Document control

Version history

Version	Date	Change
1	2026-11-06	Initial report

Distribution

TLP:CLEAR Disclosure is not limited, subject to copyright.

Data handling

Captures and reports are stored in Amazon S3 in the us-west-2 region. Uploads without an account and their reports are deleted 24 hours after upload; account reports are kept for 30 days, or for as long as a Pro subscription lasts.

Support: info@pcapai.com

SAMPLE

Contents

1 Executive summary **4**

2 Scope, evidence and limitations **5**
2.1 Evidence integrity . . . 5
2.2 Versions . . . 5
2.3 Limitations . . . 5

3 Findings summary **5**

4 Detailed findings **6**
4.1 F01: The clients of 195.81.202.68 (ES, GTT Communications Inc.):80 stopped accepting data (1 Zero Window episode, 23.7 s stalled) . . . 6

5 Remediation roadmap **6**
5.1 Immediately . . . 6
5.2 Strategic . . . 6

6 Coverage: checked and clean **7**

7 Assets and communications **7**
7.1 Asset inventory . . . 7
7.2 External destinations . . . 8

8 Capture quality and mode metrics **8**
8.1 Endpoints with problems . . . 8

9 Next capture guidance **8**

A Appendices **9**
A.1 Event log . . . 9
A.2 Methodology and scoring . . . 9
A.3 Vocabulary . . . 9

SAMPLE

Executive summary

`tcp_zerowindowdead.pcapng`
3 Mar 2009 · 15:55:16–15:55:40 UTC · 23.7 s

High | High confidence

A client cannot keep up with incoming data

The clients of `195.81.202.68` (ES, GTT Communications Inc.):80 advertised a zero receive window 1 time, pausing the sender for 23.7 s in total.

Affected: 195.81.202.68

NETWORK IMPACT

75 /100 **Impaired**

0 40 75 90

FINDINGS · 1

Critical 0 | High 1 | Medium 0 | Low 0 | Info 0

COVERAGE · 11 AREAS

1 with a finding | 2 pass | 8 not assessed

Not assessed: 1 TCP session already...

8	1	2	1	1	12
frames	flow	hosts	protocol	destination	checks run

The fault lies with the clients

Figure 1 · section 4.1

Where the fault lies



Events of the top incident, in time order

UTC

15:55:16 UTC Receive windows

Recommended actions

Immediately	The receiving application on the client is not reading...	Endpoint / IT Operations
Immediately	Check socket receive buffers and antivirus/DLP...	Endpoint / IT Operations
Strategic	Capture again and re-run the analysis	Network Operations

Capture point: not determined (low). Figures use all 8 frames. Limitations: section 2.3.

SAMPLE

2 Scope, evidence and limitations

The analysis covers tcp_zerowindowdead.pcapng (2.2 kB, 8 frames) from 2009-03-03 15:55:16.488 UTC to 2009-03-03 15:55:40.220 UTC (23.7 s).

2.1 Evidence integrity

File	`tcp_zerowindowdead.pcapng`
Size	2.2 kB
SHA-256	`202180ddbef50c3e3f068eb22f573917ad27273e6af30c9b7d77129f6aefa1e3`
Format	pcapng
Link types	ethernet
Snapshot length	65,535
Frames	8
Capture point	Not determined
First packet	2009-03-03 15:55:16.488 UTC
Last packet	2009-03-03 15:55:40.220 UTC

2.2 Versions

Engine	PcapAI Analysis Engine 0.2.0 · ruleset 2026.10.1
Content	2026.10.1 (`sha256:f246f84c4791dd30`)
ATT&CK	19.2
Intelligence lists	service categories 2026-10-09.1; GeoLite2 Country 2026-02-17; GeoLite2 ASN 2024-07-29

2.3 Limitations

- The capture point could not be determined, so every check is read as if its frames were visible.
- 8 coverage areas were assessed partly or not at all; section 6 names the missing inputs.
- Host activity outside this capture (processes, logons, other network segments) is not visible.

3 Findings summary

ID	Title	Severity	Confidence	Roles	First seen	Status
F01	The clients of 195.81.202.68 (ES, GTT Communications Inc.):80 stopped accepting data (1 Zero Window episode, 23.7 s stalled)	High	High	Affected `195.81.202.68`	2009-03-03 15:55:16 UTC	Open

SAMPLE

4 Detailed findings

4.1 F01: The clients of 195.81.202.68 (ES, GTT Communications Inc.):80 stopped accepting data (1 Zero Window episode, 23.7 s stalled)

High Network problem · Open · Confidence: High · Reference PCAI-2026-1106-8HSK-F01

The clients of `195.81.202.68` (ES, GTT Communications Inc.):80 advertised a zero receive window 1 time, pausing the sender for 23.7 s in total.

Affected	`195.81.202.68` · ES, GTT Communications Inc. · port 80
First seen	2009-03-03 15:55:16.488 UTC (T+0.000 s)
Last seen	2009-03-03 15:55:16.488 UTC (T+0.000 s)

Evidence

- A zero window means the receiving application is not reading from its socket (CPU, disk or a blocked thread); the network is not the bottleneck here.
- Zero Window episodes: 1
- Total stall: 23732 ms

Remediation: A01 (Immediately, Endpoint / IT Operations); A02 (Immediately, Endpoint / IT Operations); A03 (Strategic, Network Operations)

5 Remediation roadmap

5.1 Immediately

ID	Step	Owner	Effort	Verification	Findings
A01	The receiving application on the client is not reading data fast enough: check CPU, disk and application thread pools on that host.	Endpoint / IT Operations	Small	No Zero Window advertisements in a new capture under the same workload.	F01
A02	Check socket receive buffers and antivirus/DLP inspection on the receiving host. Linux `sysctl net.ipv4.tcp_rmem`	Endpoint / IT Operations	Small		F01

5.2 Strategic

ID	Step	Owner	Effort	Verification	Findings
A03	Capture again after applying the steps and re-run the analysis.	Network Operations	Small	The new capture shows none of these problems.	F01

SAMPLE

6 Coverage: checked and clean

What this capture let the engine check:

- **Checks:** 12 of 100 checks ran, in 3 of 11 areas; the table below gives the reason for each one that could not run.
- **Decoded:** no application protocol was recognized.
- **Hosts:** 2 hosts, 1 destination outside the network (section 7).
- **Protocols:** 1 protocol; in cleartext: HTTP (TCP/80).
- **Passwords:** no login exchange in the capture, and no credential was sent readable.
- **TLS:** no TLS handshake in the capture.

Area	Checks evaluated	Checks matched	Not run	Status	Reason
TCP connections	0	0	9	Not assessed	1 TCP session already open when the capture started; no new connections to judge
Packet loss	0	0	8	Not assessed	Only 1 TCP data packet: too little to judge loss
Latency	0	0	4	Not assessed	No complete TCP handshakes to measure round-trip time
Receive windows	5	1	0	High F01	
DNS	0	0	14	Not assessed	No DNS queries in the capture
DHCP	0	0	7	Not assessed	No DHCP exchanges in the capture
LAN (ARP, broadcast, switching)	0	0	13	Not assessed	No broadcast or ARP traffic in the capture
Routing and MTU	2	0	0	✓ Pass	
TLS	0	0	6	Not assessed	No TLS handshakes in the capture
Applications and services	0	0	27	Not assessed	No application service endpoints identified
Capture quality	5	0	0	✓ Pass	

7 Assets and communications

The capture holds 1 flow (by addresses, ports and protocol) between 1 address pair.

7.1 Asset inventory

2 internal hosts, from IP traffic, ARP, Ethernet senders and the entities of the findings.

IP	MAC	Hostname	Roles	Bytes sent	Bytes received	Risk
172.31.136.85	00:16:35:a4:c1:c6 (Hewlett Packard)	not observed		264 B	1.6 kB	
not observed	00:0b:be:72:15:00 (Cisco Systems, Inc)	not observed		0 B	0 B	

SAMPLE

7.2 External destinations

1 external destination exchanged traffic with internal hosts. Bytes are summed over its conversations; out counts the bytes the internal hosts sent.

Names come from HTTP Host, TLS SNI and DNS answers, the network owner from the GeoLite databases and the reputation from the service-category lists; section 2.2 dates each source.

Destination	Network owner	Protocol	Internal hosts	Reputation	Bytes out (conversations)	Bytes in (conversations)
195.81.202.68	AS3257 · GTT Communications Inc. · ES	HTTP (TCP/80)	172.31.136.85	Not listed	264 B	1.6 kB

8 Capture quality and mode metrics

Capture point	Not determined: The 8 frames of unicast IP traffic between local hosts are too few to tell.
Position on the TCP paths	Undetermined
Frames cut by the snapshot length	0
Packets dropped by the capture tool	not reported
Segments acknowledged but not captured	0
Duplicate frames (captured twice)	0
One-sided TCP sessions	0 of 1
Network health impact	75 of 100
Network issues found	1
TCP retransmissions	0
Estimated packet loss	0.0%
Time stalled by zero receive windows	23,732 ms

8.1 Endpoints with problems

Endpoint	field-role	Service	Failed connections	Retransmissions	Loss	Median RTT	Status
195.81.202.68 (ES, GTT Communications Inc.):80	server	HTTP (TCP/80)	0 of 1	0	0.0%	not measured	stalled

9 Next capture guidance

Why a new capture would help

- The capture is shorter than 5 minutes.
- The capture point could not be determined.
- Some areas could not be assessed because their protocols were absent.

How to capture

- Capture on a SPAN port or TAP of the gateway uplink or the server segment.
- Capture for at least 15 minutes, ideally during business hours.
- Use the full snapshot length.
- Do not use capture filters that drop ARP, DNS or DHCP.

SAMPLE

A Appendices

A.1 Event log

Time (UTC)	ID	Observation
2009-03-03 15:55:16.488 UTC T+0.000 s	F01	First seen: The clients of 195.81.202.68 (ES, GTT Communications Inc.):80 stopped accepting data (1 Zero Window episode, 23.7 s stalled)

A.2 Methodology and scoring

Detection rules inspect captured protocol data. Findings with the same rule and key entities are merged; the report lists them in order of severity, confidence and first appearance.

Confidence follows fixed rules. High: the primary signal, every required check passes, at least one strong check passes and no alternative remains open. Medium: the primary signal, no required check fails, and either no strong check passes or an alternative remains open. Low: a partial primary signal, or a required check could not be evaluated.

Each finding scores its severity weight (Critical 90, High 75, Medium 45, Low 20) times a confidence factor (High 100%, Medium 85%, Low 60%); exposures are capped at 75 and indicators at 40. Overall risk is the highest finding score plus at most 15 points for attack breadth across tactics, affected hosts and linked findings. Bands: Low 0-24, Guarded 25-49, Elevated 50-74, Severe 75-100.

A host's risk is the highest score of the findings that name it, weighted by its role (suspected source 100%, affected or impersonated 80%, client or server of an exposure 70%), plus 3 points for each further finding, at most 10, capped at 100.

Every observation lists the Wireshark frames it rests on and a display filter that selects them in the original capture.

Framework references list the controls to review for each finding. They do not state compliance or non-compliance; applicability depends on the organization's scope.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique, tactic and mitigation names come from ATT&CK 19.2, © The MITRE Corporation, used under its terms of use.

A.3 Vocabulary

- Threat: activity that indicates an attack in progress or completed.
- Exposure: a weakness that could be used against the network; no attack on it was observed.
- Indicator: a signal worth reviewing; on its own it is not evidence of an attack.
- Severity: Critical, High, Medium, Low or Info, set by the finding profile and its conditions.
- Confidence: High, Medium or Low, set by the automatic checks listed on each finding.
- Risk bands: Low 0–24, Guarded 25–49, Elevated 50–74, Severe 75–100.
- Frame: one captured packet, numbered as in Wireshark.
- Conversation: all traffic between two IP addresses, in both directions, as in the Wireshark IPv4 and IPv6 conversation statistics.
- TCP session: one TCP connection.
- Exchange: one request with its response.
- Observation: one evidence row of a finding, with its frames and display filter.
- Check: one detection rule evaluated on the capture. Area: the checks of one attack family.
- Host: an internal device of the asset inventory. Destination: an external address that exchanged traffic with internal hosts.
- Bytes: out is sent by the internal host and in is received by it. Request and response bytes count the application message; conversation bytes count whole frames.

SAMPLE