Edge of Compromise:

The Ivanti Connect Secure Exploit Chain (Dec 2024–Jan 2025)

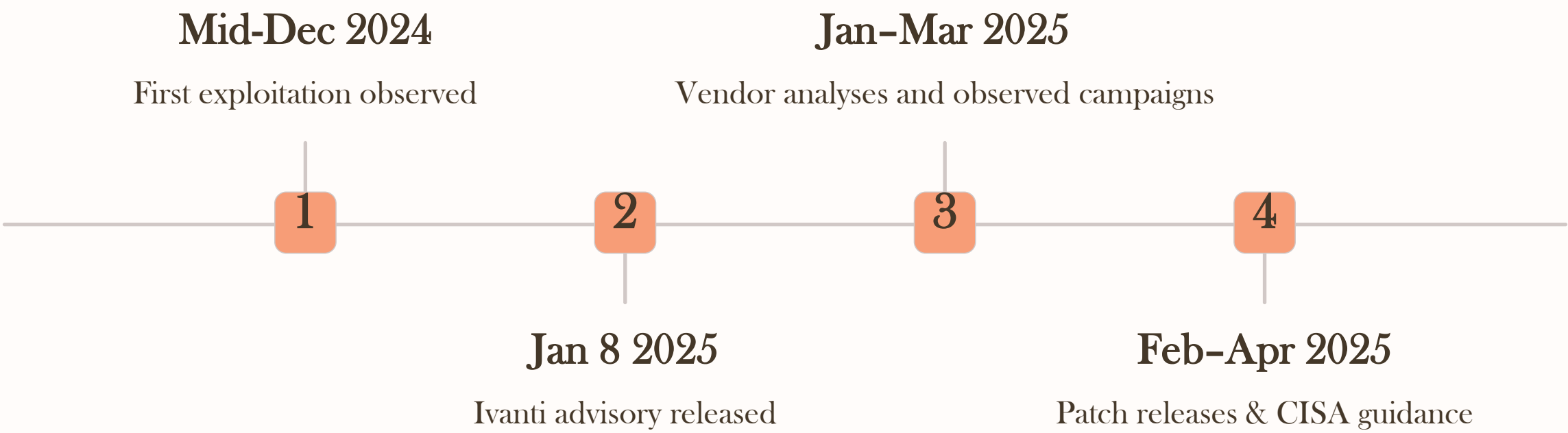
Name: Bishnu Prasad Kar
edX Username: BP_2506_OW25
GitHub Username: Bishnu2430
Recording Date: 10 October 2025
Incident month/year: January 2025
CVE(s): CVE-2025-0282, CVE-2025-0283

Ivanti Connect Secure Exploit Chain Overview

- Unauthenticated remote code execution (CVE-2025-0282 / CVE-2025-0283) in Ivanti Connect Secure was observed exploited in the wild in Dec 2024–Jan 2025.
- Attackers deployed fileless, in-memory loaders and backdoors, harvested credentials/certificates, and pivoted from the appliance into internal networks.
- Vendor advisories and emergency patches were released (Jan–Apr 2025); defenders must prioritize patching, isolation, and credential rotation.

Timeline of the Ivanti Vulnerability Exploitation

The timeline below illustrates the critical period between initial exploitation and the availability of comprehensive patches.



Citations: Google Cloud, 2forums.ivanti.com, Google Cloud

The gap between initial exploitation and patch rollouts highlights the challenge of zero-day defense.

Vulnerability Details

Critical Vulnerabilities

- CVE-2025-0282 (stack buffer overflow → unauth RCE)
- CVE-2025-0283 (auth/logic flaw)

A stack buffer overflow is a critical flaw where a program writes more data to a buffer located on the stack than it was intended to hold. Unauthenticated RCE (Remote Code Execution) is critical because it allows an attacker to execute arbitrary code on the target system without needing valid credentials.

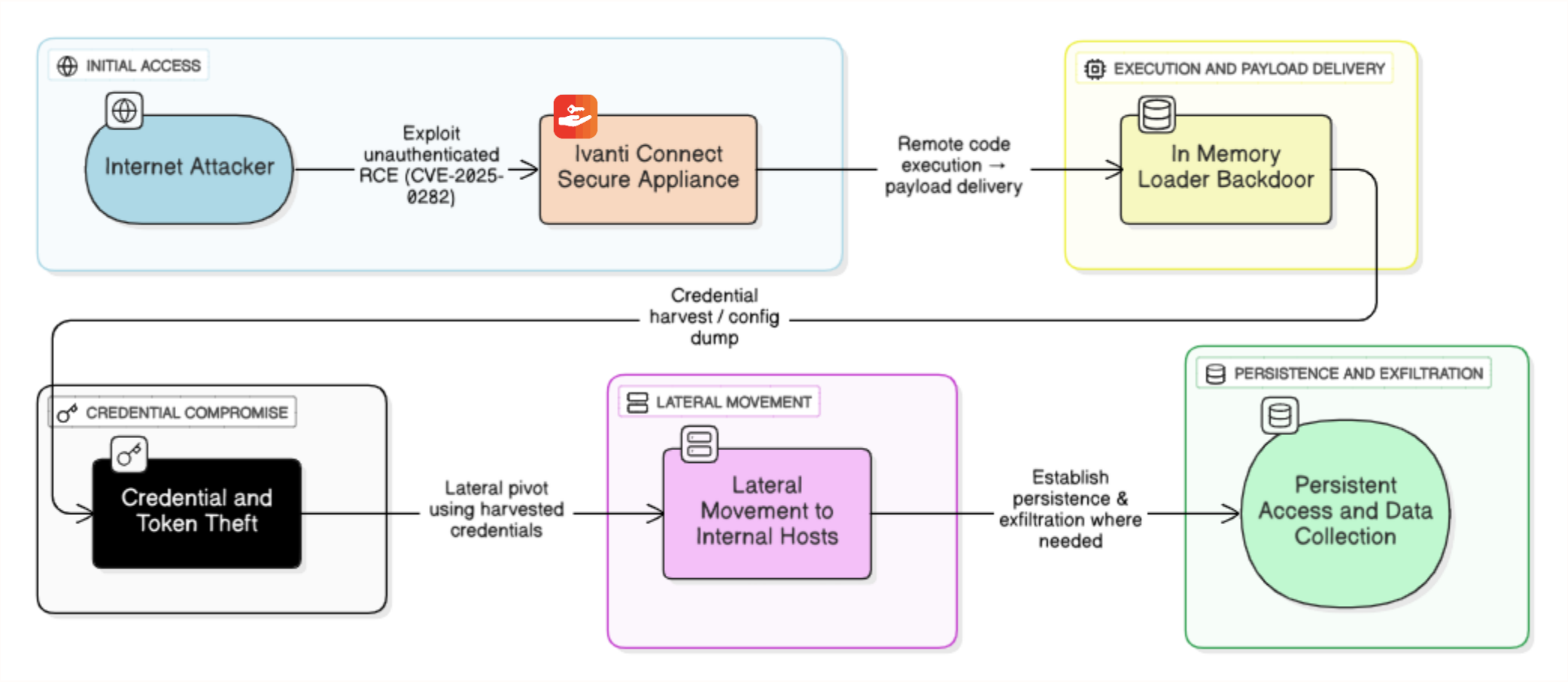
Affected Modules and Versions

The following versions are vulnerable (copy versions directly from Ivanti advisory):

- Ivanti Connect Secure (ICS) 9.x and 22.x prior to 22.5R2.2
- Ivanti Policy Secure (IPS) 9.x and 22.x prior to 22.5R2.2
- Ivanti ZTA Gateways prior to 22.5R2.2

Source: forums.ivanti.com

Attack Chain Flowchart



Source: Google Cloud

The attack begins with initial access, followed by the exploitation of CVE-2025-0282 and CVE-2025-0283. This leads to fileless payload delivery, credential harvesting, and ultimately lateral movement and persistent access within the network.

Payload & TTPs Observed

In-Memory Loaders

These are fileless payloads, meaning they reside only in memory, making traditional file-based detection difficult.

Backdoors (Beaconing)

Malicious implants establish persistent communication channels (beaconing) to command-and-control servers.

Credential Harvesting

Attackers actively seek to steal user credentials for further access and lateral movement.

Lateral Movement

Once inside, the attackers move across the network to reach high-value targets.

Malware names reported (observed in some cases) include TRAILBLAZE, BUSHFIRE, and SPAWN. These TTPs complicate detection because they bypass standard endpoint security measures and rely on stealthy network activity.

Source: TechRadar

Evidence & Indicators (IOCs and Logs to Check)

Security teams must actively search for these indicators of compromise (IOCs) in their logs and SIEM systems.

- **Unusual outbound connections from ICS IPs**

  Look for connections to rare or suspicious external IP addresses or domains.

- **Admin console logins from appliance IP**

  Monitor for administrative access originating from the appliance itself, which is highly suspicious.

- **SIEM Query Example**

  `process_name: <appliance_process> AND child_process: unexpected`

- **IntegrityChecker alerts (Ivanti tool)**

  Any alerts from the vendor-provided tool should be treated as high-priority incidents.

Tune thresholds to detect subtle anomalies. Refer to Unit42/Mandiant for detailed IOC types.

Source: Unit 42

Mitigations: Immediate & Medium Term

Prioritization is key: patch first, and if immediate patching is impossible, block access and monitor aggressively.

Patch Appliances Immediately

Apply all available vendor patches as the highest priority action.

Isolate Admin Ports

Isolate internet-facing admin ports to reduce exposure.

Rotate Credentials & Certificates

Assume compromise and rotate all associated credentials and certificates.

Deploy EDR/SIEM Rules

Implement network egress filtering and deploy specific detection rules.

Use IntegrityChecker

Run the vendor IntegrityChecker tool to scan for signs of compromise.

Source: forums.ivanti.com, Ivanti Forums

Detection Playbook for SOC Teams

A structured approach is necessary to handle potential compromises effectively.

01

Triage Alerts

Immediately investigate any alerts related to the appliance or unusual network activity.

02

Collect Volatile Memory

Capture volatile memory from the appliance for forensic analysis.

03

Snapshot Configs & Rotate Keys

Preserve current configurations and rotate all associated keys.

04

Run IntegrityChecker & Search SIEM

Execute the vendor tool and perform deep SIEM searches using known IOCs.

Sample SIEM Query Template:

```
event_type=network_connection AND
destination_ip=IOC_IP
```

Source: Unit 42

05

Escalate & Notify

Escalate findings to the Incident Response (IR) team and notify affected stakeholders.

Course Tie-ins & Lessons Learned

This incident provides real-world context for several key course topics:

- Vulnerability lifecycle
- Exploit chaining
- Incident response
- Supply-chain risk
- Patch management

Three Short Lessons for Defenders

Zero-Day Readiness

Assume internet-facing devices will be targeted and have a rapid isolation plan ready.

Defense in Depth

Relying solely on perimeter security is insufficient; focus on internal detection (fileless payloads).

Proactive Integrity Checks

Regularly use vendor-provided integrity tools, even before an advisory is released.