Research on CVE-2025-9998

CVE-2025-9998 is a medium-severity vulnerability found in the networking server component of ARC Informatique's PcVue SCADA software, and it is regarded as a particularly serious risk for industrial control environments where constant operation is vital. This vulnerability is captured by CWE-754 (Improper Check for Unusual or Exceptional Conditions), meaning the application fails to robustly validate the order and logic of incoming network packets, which can lead to denial-of-service (DoS) conditions if exploited by a threat actor.

Technical Background and Roots of vulnerability ,the affected feature within PcVue is the TCP-based client-server networking functionality, employed to transfer real-time process information, control messages, and system status data between remote SCADA workstations. In safe operation, every network message (packet) must progress in a predictable order as per the design of the protocol; variations like out of order, duplicate, or malformed packets must be recognized and safely discarded. But in all previous versions of PcVue up to 16.3.1, 15.2.12, and 12.0.31, the network server does not properly check for such out of band conditions and thereby usually does not detect or process protocol violations in its message stream. When a malicious user with access to the same network segment as the PcVue server sends cleverly crafted packets specifically intended to violate protocol sequencing rules or carry unexpected types of messages the logic of the server can become unstable. Rather than writing an error or handling the event graciously, the PcVue process can simply terminate, leaving a service unavailable. This kind of invalid state transition or out of exception condition is characteristic of input validation errors in protocol logic, and in highly automated industrial settings, the consequent downtime can freeze critical monitoring, device control, or alarm handling services.

Why This Vulnerability Occurs (Incorrect Packet Sequence)

Validation Logic: PcVue's networking server expects packets to arrive in a predefined, well-ordered sequence as per its proprietary communication protocol. Each packet usually contains sequence identifiers or other ordering information that informs the application of the proper order in which to process the data. However, in affected

versions, PcVue does not thoroughly check or validate this sequencing. When packets arrive out of order or contain unexpected sequencing values (e.g, duplicated orkipped sequence numbers) PcVue attempts to process them incorrectly rather than rejecting or safely discarding them. This improper validation results in inconsistent internal state or logic errors within the packet processing routine.

Handling of Exceptional Network Conditions: TCP networks can occasionally deliver packets out of order due to retransmissions, network jitter, or connection interruptions. Well-designed network applications incorporate robust exception handling logic for such cases, ensuring that out of order packets either wait to be reordered or are discarded gracefully. PcVue implementation lacks these robust checks , leading to what the CWE-754 classification calls improper checking for unusual or exceptional conditions. When exceptional conditions occur, PcVue doesn't just log or correct these they cascade and lead to fatal errors, such as memory access violations or corrupted internal data structures.

Race Conditions and Potential Memory Corruption: The error handling for packets in unexpected states may trigger race conditions or unsafe memory operations inside PcVue's networking stacks. For example, the handling of out of order sequences or duplicated packets without proper synchronization can cause memory to be referenced more than once or freed improper. Such low level flaws disrupt the normal operation of the networking server thread or process, which ultimately causes the PcVue application to crash or stop altogether.

Lack of Defensive Programming in Protocol Layers: Industrial SCADA software such as PcVue relies heavily on consistent and reliable communication between multiple networked components. Many protocols integrate sequence numbers, checksums, and acknowledgement packets to verify data integrity and correct delivery order. PcVue's code for managing these protocol features appears to insufficiently enforce these integrity checks, lacking adequate input sanitization and boundary validations at critical points in the networking code path. This insufficient defensive coding leaves the software open to attacks that craft unusual targeting these weaknesses.

Complexity of Industrial Network Protocols: The underlying

communication protocols used by PcVue in the SCADA environment tend to be custom or specialized for control system scenarios, where reliability and real time responses are prioritized. This increases the challenge of ensuring error and makes it easy for corner cases like unusual packet sequences to be overlooked during development or testing phases. Legacy and proprietary protocols commonly face this issue because their state machines must manage numerous network edge cases that are hard to simulate and validate extensively.

Vulnerability solution

The definitive solution to the CVE-2025-9998 vulnerability lies in applying the official vendor patches released by ARC Informatique. The vulnerability stems from improper validation of packet sequencing in PcVue's TCP-based networking server, and the only permanent fix involves updating to versions where this logic is corrected.

1.Apply Vendor-Published Patches: ARC Informatique has issued fixed releases for all affected product branches to address this vulnerability:

- Upgrade PcVue 16.x to version 16.3.1

- Upgrade PcVue 15.x to version 15.2.12

- Upgrade PcVue 12.x to version 12.0.31

It is critical that patches be installed on all PcVue stations in the network simultaneously. If some stations remain on vulnerable versions, communication between patched and unpatched stations will fail, potentially causing network-wide disruptions.

2. Harden Network Configuration: Until patching is completed, mitigation of risk is achievable by reducing exposure to malicious traffic[1]:

- Isolate the PcVue control system network using firewalls, so it is not accessible from external or corporate networks unless strictly necessary.

- Use network segmentation and place PcVue servers behind well-configured perimeter firewalls.

- Restrict traffic to known, trusted hosts and authorized ports used by PcVue networking.

3. Restrict Remote Access : When remote access to the network is needed, use secure methods like VPNs with the latest updates and best practices. Even then, understand that VPN security relies on the security of connected endpoints; therefore, continually secure and monitor those hosts.

4. Monitor Traffic for Suspicious Activity: Deploy intrusion detection and prevention systems that specifically look for anomalies matching malformed or out-of-sequence packet transmissions to PcVue servers. Real-time alerts on such traffic can provide early warnings of exploitation attempts[1].

5. Implement Defense in Depth:

- Use local host firewalls to limit traffic on PcVue servers to only essential services and ports.

- Ensure all other PcVue and system software components are kept up to date.

- Maintain good logs and monitor for repetitive crashes or unusual network communication patterns.

6. Operational Best Practices:

- Establish redundancy and failover to mitigate impact of any one node crash.

- Document patching and network policies clearly to maintain consistent security posture.

- Conduct security awareness training focused on SCADA cybersecurity hygiene.

Fully resolving CVE-2025-9998 requires upgrading PcVue to fixed versions provided by ARC Informatique where the packet sequence validation is properly implemented and tested. Supplementing updates with network defenses, access controls, and monitoring provides comprehensive risk mitigation and helps defend critical infrastructure against denial-of-service attacks exploiting this vulnerability.

Vulnerability solution with help of artificial intelligence

Artificial Intelligence (AI) can play a significant role in solving or mitigating vulnerabilities like CVE-2025-9998 in industrial control systems such as PcVue SCADA software by enhancing detection, prevention, and response capabilities.

1.Real-Time Anomaly Detection in Network Traffic: AI powered network monitoring systems use machine learning to continuously analyze network traffic patterns and detect anomalies, including unusual packet sequencing or malformed packets that exploit CVE-2025-9998. By learning normal communication behavior in PcVue networks, AI models can identify abnormal sequences or patterns indicative of an attack and raise instant alerts or automatically block suspicious traffic.

2.Predictive Threat Intelligence: Machine learning algorithms can analyze historical attack data and vulnerability patterns to predict potential exploitation attempts. This proactive approach helps operators to prioritize patching and take preemptive defense measures before vulnerabilities are exploited in the wild.

3. Automated Incident Response: AI-driven security systems can implement automated defense actions, such as isolating PcVue servers if unusual packet sequences are detected, or temporarily blocking suspicious network connections to limit the attack surface. This reduces the risk of service disruption while operators investigate and mitigate the issue.

4. Continuous Vulnerability and Patch Management: AI tools can assist by scanning the OT environment to identify all PcVue instances and assess their patch status. By correlating vulnerability databases and providing actionable reports, AI helps ensure timely deployment of security patches that fix vulnerabilities including CVE-2025-9998.

5. Reducing False Positives: Conventional intrusion detection systems suffer from high false alarm rates. AI models improve signal-to-noise ratios by better distinguishing genuine malicious sequences from benign network anomalies, thus focusing attention where it is truly needed without overwhelming security personnel.

6.Adaptive Learning and Evolving Defenses: AI powered systems continuously learn from new network traffic and attack attempts, adapting their models to emerging threats or changed environments. This reduces the window of vulnerability as attacks evolve in sophistication.

By employing AI-based anomaly detection, predictive analytics, and automated incident response, organizations can significantly enhance their ability to detect, prevent, and mitigate attacks that exploit packet sequencing vulnerabilities like CVE-2025-9998. In parallel with prompt patching and network security hardening, AI-driven solutions represent a powerful tool in protecting critical industrial control systems against evolving cyber threats.