



Strategic Security Review

Created for Acme Financial
Prepared by: Nick Bartosh





Readout

1

The VulnCheck Value

2

What was found

3

Why it matters

4

Prioritized Action Plan

5

VulnCheck Enrichment

Overview

Acme Financial Provided VulnCheck with a subset of CPEs that are representative of devices they own and maintain.

Request: Assess CVEs associated with the provided CPEs. Provide feedback, recommendations and next steps based on documented results.



The VulnCheck Value



Risk Reduction

- Prioritize vulnerabilities based on **real exploitation evidence**
- Focus remediation efforts on **what actually matters**
- Provide **clear evidence to leadership and auditors** on the WHY

Vulnerability Management

- Shift from a reactive to approach to **proactive strategic risk control** cadence
- Enables **risk based decision making** to filter out noise
- Measurable improvements in **MTTR for exploited vulnerabilities**

Early Warning

- Receive **early warning signals** when vulnerabilities move from disclosure to exploitation
- **Near real-time intelligence** allows teams to stay ahead of adversaries and focus on what matters
- **Prioritized intelligence** on critical banking assets









Operational Alignment

- **Integrates into existing workflows** rather than requiring new processes
- **Align security, IT, Engineering and GRC** with the same prioritized risk signals
- Translates technical vulnerabilities into **clear, exploitation-driven narratives**

What was Found



Vulnerabilities by Asset

 Palo Alto Firewall	Critical		cpe:2.3:o:paloaltonetworks:pan-os:11.2.4:h2:*:*:*:*:*	C: 1	H: 4	M: 8	L: 1	▼
 Windows Server	High		cpe:2.3:o:microsoft:windows_server_2025:10.0.26100.4946:*:*:*:*:x64.*	C: 3	H: 174	M: 74	L: 3	▼
 Ivanti Gateway	Critical		cpe:2.3:a:ivanti:virtual_traffic_management:22.7:r1:*:*:*:*:*	C: 1	H: 0	M: 0	L: 0	▼
 Smart HMI	High		cpe:2.3:a:smart-hmi:webiq:2.15.9:*:*:*:*:*	C: 1	H: 0	M: 0	L: 0	▼

Why it Matters



Not all vulnerabilities are equal.

The highlighted vulnerabilities are being activated exploited by adversaries and have an EPSS score of over 60%. This means that there is a strong possibility you will experience an attack in the next 30 days for each of these CVEs.

Out of over 270 open vulnerabilities associated with the provided devices, the 5 below represent real, present risk to the organization and should be prioritized for remediation / mitigation efforts.

Palo Alto Firewall

CVE-2024-0012
CVE-2025-0108

Ivanti Gateway

CVE-2024-7593

Windows Server

CVE-2025-59287

Smart Workstation

CVE-2024-8752

CVEs



Palo Alto Firewall

- **CVE-2024-0012** - An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain PAN-OS administrator privileges to perform administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities
- **CVE-2025-0108** - An authentication bypass in the Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to bypass the authentication otherwise required by the PAN-OS management web interface and invoke certain PHP scripts. While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS.

CVEs



Ivanti Gateway

- **CVE-2024-7593** - Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

CVEs



Windows Servers

- **CVE-2025-59287** - Deserialization of untrusted data in Windows Server Update Service allows an unauthorized attacker to execute code over a network.

CVEs



Smart Workstation

- **CVE-2024-8752** - The Windows version of WebIQ 2.15.9 is affected by a directory traversal vulnerability that allows remote attackers to read any file on the system.

Prioritized Action Plan



1

Palo Alto Firewall

- Update WAF rules
- Immediately patch or upgrade device
- Verify mgmt interface is only available on the internal network and only to trusted IPs
- Review logs for signs of exploitation
- Reset passwords
- Update signatures to monitor for IOCs

2

Ivanti Gateway

- Update WAF rules
- Immediately patch or upgrade device
- Verify mgmt interface is only available on the internal network and only to trusted IPs
- Review logs for signs of exploitation / unauthenticated access
- Reset passwords
- Update signatures to monitor for IOCs

3

Windows Servers

- Verify WSUS server role is disabled
- **If WSUS is NOT disabled**
Block inbound traffic on ports 8530, 8531
- Patch server with October 23, 2025 OOB update ASAP

4

Smart HMI

- Review ACLs to include directory traversal mitigations
- Verify the PURDUE model for OT access is followed
- Review access policies if connected to enterprise network

VulnCheck Enrichment



- **Correlated vulnerabilities using CPEs (/cpe)**
 - 270 vulnerabilities associated to provided CPEs
 - Single API Call to VulnCheck vs calls to several endpoints
- **Enriched CVE Data in a single location (/index/vulncheck-nvd2)**
 - Aggregated / Authoritative source for CVE Data
 - Standardized outputs
- **Exploit Enrichment (index/exploits)**
 - Active intelligence on Ransomware, Botnets, Threat Actors
 - Links to POCs and exploits
 - Initial access detection (canaries)
- **Risk Prioritization**
 - EPSS Scoring to document likelihood as well as severity
 - Evidence Based Vulnerability Prioritization model
- **Aggregated CVE Data from thousands of disclosure sources for up-to-date**



Thank you.

