NeoPay Threat Intelligence

WE Innovate X Zero$ploit

Supervised by : Muhammed Badawy

Threat Intel Team :

Omar Hassan – Ali Abdelrahman – Ahmed Taha – Omar Tarek – Rami Khaled –Noha Sayed

Who are NeoPay ?

NeoPay *is a fast-growing* ***FinTech company*** *based in Cairo, providing digital payments, mobile wallets, and Open Banking services across the MENA region.*

Core Business Functions:

- *Processing online payments for e-commerce merchants.*
- *Managing consumer accounts and transactions via the NeoWallet mobile app.*
- *Providing regulated Open Banking data access to partner institutions.*
- *Handling sensitive customer data (PII, financial records).*

Topics Covered

1. **Vulnerability Assessment**
   - *1.1. Web Applications*
   - *1.2. API's & Services*
   - *1.3. Infrastructure*
   - *1.4. Endpoints*
   - *1.5. 3rd Party Dependencies / Vendors*

2. **Incident Analysis**
   - *2.1 Ransomware*
   - *2.2 Phishing*

3. **Recommendations (Mitigation Actions)**

Vulnerability Assessment

Web Application

After scanning our web application platform ***Ali Abdelrahman*** *found this :*

Apache Tomcat 10.1.X

- **CVE-2025-24813** – Critical Remote Code Execution via Partial PUT
  Exploit via ***partial PUT + default servlet write + file-based sessions*** *→ arbitrary code execution*

- **CVE-2024-50379** – Race Condition RCE

*JSP compilation **race condition** on case-insensitive FS when servlet write enabled*

- **CVE-2025-31651** – Denial of Service (DoS)
  *Attackers bypass **rewrite rules**, possibly subverting constraints → DoS*

CVE	Severity	Score
CVE-2025-24813	***Critical***	*9.8*
CVE-2024-50379	***High***	*8.2*
CVE-2025-31651	***High***	*7.5*

API's & Services

*By checking the API & services **Rami khaled** found this :*

- **CVE-2025-7784** - (Keycloak Privilege Escalation)
  *Users with limited roles (manage-users) can **escalate privileges to realm-admin**, leading to full takeover of identity management.*

- **CVE-2024-9666** - (Keycloak DoS via Proxy Header Abuse)
  ***Abuse of unvalidated proxy** headers can overload DNS resolution, causing denial of authentication services.*

- **CVE-2023-34055** - (Spring Boot Actuator DoS)
  *Crafted HTTP requests to Actuator endpoints can **degrade or crash applications** using Spring Boot with Actuator.*

CVE	Severity	Score
CVE-2025-7784	***High***	*7.5*
CVE-2024-9666	***Medium***	*Not Specified*
CVE-2023-34055	***Medium***	*5.3*

Infrastructure

*After analyzing the infrastructure **Noha elsayed** found this :*

- **CVE-2025-7342** – Kubernetes Image Builder Default Credentials
  *Default credentials left in images (Nutanix/OVA) allow attackers to **log into new nodes and access workloads.***
- **CVE-2025-5690** – PostgreSQL Anonymizer Masking Bypass
  *Masking rules in PostgreSQL Anonymizer v2.0/v2.1 can be bypassed, **exposing sensitive data** (e.g., credit card numbers).*

- **CVE-2025-4207** – PostgreSQL Multibyte Encoding Buffer Over-Read
  *Malformed multibyte input can crash PostgreSQL, **causing denial of service**.*

CVE	Severity	Score
CVE-2025-7342	***High***	*7.5*
CVE-2025-5690	***High***	*7.5*
CVE-2025-4207	***Medium***	*6.5*

Endpoints

*After analyzing the endpoints on the network **Omar Hassan** found this :*

- **CVE-2025-33073** – Windows SMB Client Elevation of Privilege
  *A flaw in the Windows SMB client allows low-privileged attackers to **gain SYSTEM-level access** over a network without user interaction—threatening full system compromise*

- **CVE-2025-29966** – Windows Remote Desktop Services (RDP) Remote Code Execution
  *This critical RCE vulnerability in RDP enables attackers to **execute arbitrary code remotely** on Windows systems without authentication, risking endpoint takeover.*

- **CVE-2025-53731** – Microsoft Office Remote Code Execution (e.g., via Preview Pane)
  *A remote code execution vulnerability in Microsoft Office that allows unauthenticated attackers to **run arbitrary code through crafted documents**—especially via the Preview Pane.*

CVE	Severity	Score
CVE-2025-33073	***High***	*8.8*
CVE-2025-29966	***High***	*8.8*
CVE-2025-53731	***High***	*8.4*

3rd Party Dependencies / Vendors

*After investigating the 3rd party vendors used by **NeoPay** , **Ahmed Thabet & Omar Tarek** found this :*

- **CVE-2025-30066 -** GitHub Actions "tj-actions/changed-files" Supply Chain Attack
  A malicious actor compromised the popular GitHub Action tj-actions/changed-files (versions before 46), **injecting code** that exposed secrets (e.g. API keys, access tokens) via build logs.

- **CVE-2024-9191 -** Okta Verify Agent for Windows (Passwordless Device Access)
  For Okta Verify for Windows, attackers with local device access could **exploit insecure access to the OktaDeviceAccessPipe** to retrieve passwords tied to passwordless MFA credentials.

- **CVE-2024-45401 -** Stripe-CLI Path-Traversal Vulnerability
  In Stripe's command-line interface , a **malformed plugin manifest installed** via --archive-url or --archive-path could enable arbitrary file overwriting (path traversal)

CVE	Severity	Score
CVE-2025-30066	***High***	*8.6*
CVE-2025-30066	***High***	*7.6*
CVE-2024-45401	***High***	*7.1*

Incident Analysis

Ransomware Attack

- **Impact on Operations:** *A ransomware attack could encrypt NeoPay's payment processing systems and mobile wallet infrastructure, halting transactions for merchants and consumers. This downtime would directly disrupt revenue flow and trust in the platform*.

- **Impact on Security Posture:** *It would expose weaknesses in incident response and disaster recovery planning, potentially signaling to attackers that NeoPay is a viable target for future exploitation.*

- **Impact on Customers:** *Customers may lose access to their funds, experience delayed payments, or fear data exposure, eroding confidence in NeoPay's reliability and brand reputation.*

Phishing Attack

- **Impact on Operations:** *Successful phishing against employees could result in compromised credentials, giving attackers unauthorized access to internal systems, customer accounts, or sensitive data.*

- **Impact on Security Posture:** *Phishing compromises highlight gaps in employee awareness and authentication controls, weakening overall resilience against social engineering.*

- **Impact on Customers:** *Customers targeted by phishing campaigns impersonating NeoPay may disclose financial data, leading to fraud and reputational damage for the company.*

Recommendations

1. **Implement Regular Patching and Updates**
   - Ensure all servers, mobile apps, and third-party integrations are updated promptly to reduce exploitable vulnerabilities.

2. **Strengthen Monitoring and Threat Detection**
   - Deploy a Security Information and Event Management (SIEM) system to monitor anomalies in transactions, login attempts, and system behavior in real time.

3. **Conduct Proactive Threat Hunting**
   - Establish a dedicated team to identify and contain threats early, especially focusing on ransomware indicators and phishing campaigns.
4. **Enhance Employee Awareness and Multi-Factor Authentication (MFA)**
   - Provide mandatory phishing simulations and enforce MFA for all employee and customer logins to minimize credential compromise risk.

5. **Vendor and Third-Party Risk Management**
   - Regularly assess and audit suppliers (e.g., cloud providers, payment processors) to ensure they maintain strong cybersecurity practices aligned with NeoPay's risk profile.