AMPCUS CYBER

INTELLIGENT CYBERSECURITY DELIVERED

How a Single Exposed File Led to Critical Bank System Compromise

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

PROJECT INITIATION AND SCOPING

An internal penetration test was conducted for a leading banking organization to evaluate its internal security posture. The objective was to identify vulnerabilities that could lead to data exposure or system compromise. Due to the sensitivity of the engagement, all identifying details remain confidential.

5-STEP ATTACK CHAIN

CVSS SCORE:
10.0
(CRITICAL)

DATABASES IMPACTED:
2
(ORACLE, MSSQL)

ENVIRONMENT OVERVIEW

The assessment covered internally accessible services across multiple ports. During enumeration, a service running on port 4500 was identified. Further analysis revealed that the server had directory listing enabled, exposing internal application files and directories. Several backup and legacy folders were accessible, indicating poor handling of deployment artifacts and lack of access controls.

www.ampcuscyber.com | letsconnect@ampcuscyber.com

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

ASSESSMENT METHODOLOGY AND EXECUTION

The assessment began with internal reconnaissance and service enumeration. Exploration of the exposed service led to the discovery of an API path containing a publicly accessible .env file. This file included sensitive credentials and secrets for multiple internal systems. Using the exposed credentials, access to backend databases was successfully established. The Oracle database contained highly sensitive customer information, including account numbers, passbook details, and other critical financial data. To maintain responsible testing practices, only minimal records were accessed for proof-of-concept validation, which was sufficient to confirm unrestricted database access. Further use of the same credentials allowed authentication to the MSSQL database, where additional sensitive information such as usernames, hashed passwords, and role assignments was identified. To assess the extent of the impact, system-level command execution was tested through the database service, successfully confirming remote command execution capabilities on the underlying host.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Attack Path:

- Directory listing was enabled on an internal server, which exposed multiple application directories, including backup and legacy files, allowing unrestricted access to sensitive resources.

- Within these accessible directories, a .env configuration file was discovered that contained credentials and secrets for multiple internal systems and databases.

- Using the exposed credentials, successful authentication was achieved to the Oracle database, enabling access to highly sensitive customer data such as account numbers and other highly sensitive personally identifiable information.

- The same credentials were used to authenticate to the MSSQL database, where additional sensitive data was identified, including usernames, hashed passwords, role information, and much more.

- To further assess impact, xp_cmdshell was enabled to execute system-level commands, confirming command execution on the host, after which it was promptly disabled to maintain system integrity.

The vulnerability was assigned a CVSS score of **10.0 (Critical)** due to the ability to access sensitive data and achieve system-level command execution.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

REMEDIATION SUPPORT AND RESPONSIBLE TESTING

Due to the critical nature of the findings, the issue was immediately reported.

Testing was conducted responsibly in a production environment. Only minimal data was accessed for validation, and no data was modified or exfiltrated. Any temporary changes made during testing were reverted immediately.

Any temporary changes made during testing were reverted immediately.

CONCLUSION

This case demonstrates how a single exposed file can lead to critical system compromise in a banking environment.

An attacker could extract credentials, access sensitive customer data, and execute commands on internal systems. This creates serious risks including data breaches, financial fraud, and system compromise.

It highlights the importance of securing internal services, protecting sensitive files, and enforcing strict access controls. Even a small oversight can result in a high-impact security incident.

www.ampcuscyber.com | letsconnect@ampcuscyber.com