Information Security and Risk Assessment

Project: IBM Cloud

TA: Alaa Prince

Team Members:

Makarious Magdy Azmy: 20231700340

Kerolos Ayman Ebrahim: 20231700329

Yara Tamer Kamel: 20231700343

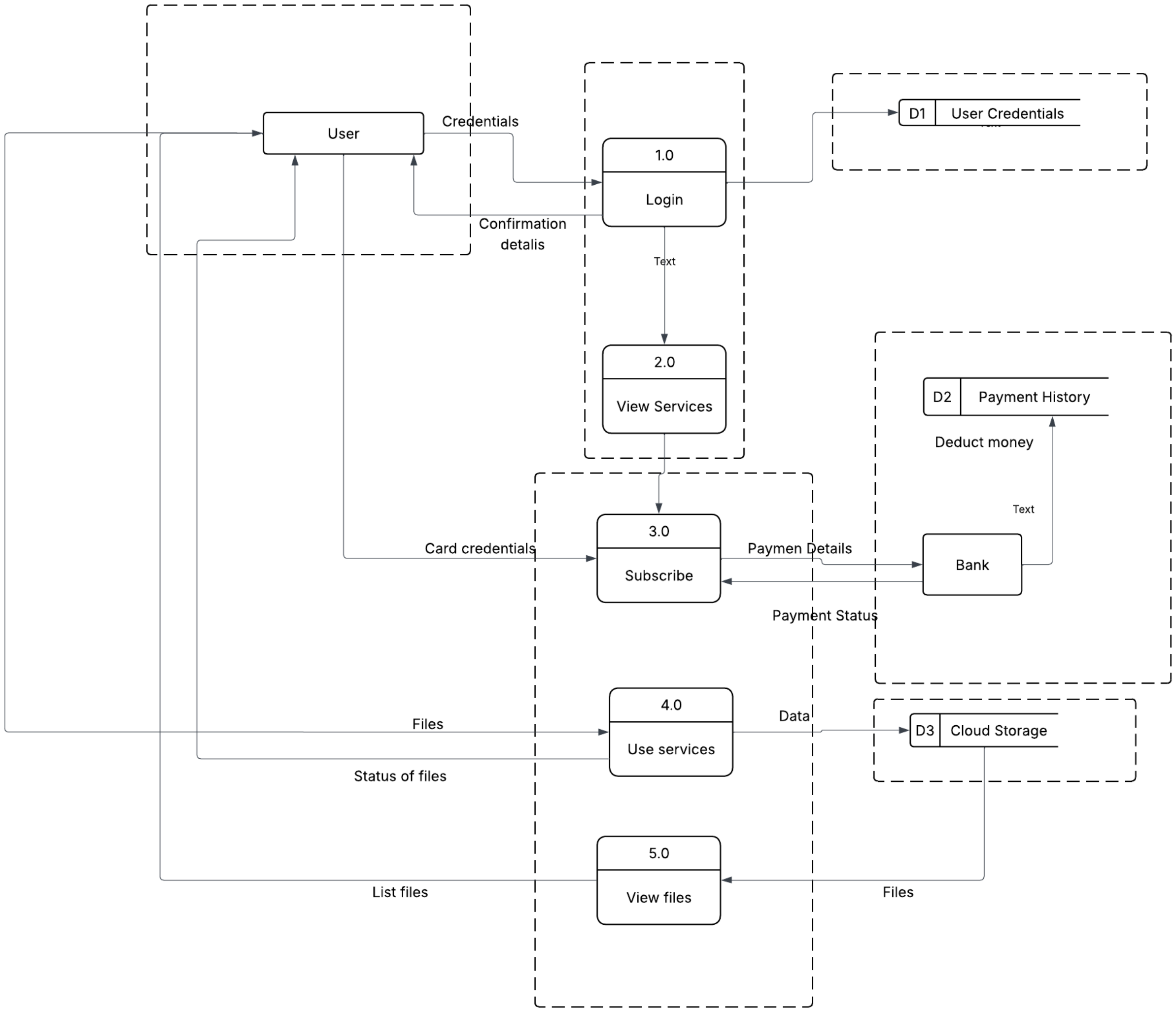
Joy Ashaf Drehem: 20231700217

Rinad Osama Mahmoud: 20231700222

Contents

Executive Risk Brief:

IBM Cloud is a cloud platform that helps organizations run and manage their applications and data over the internet. It provides services such as computing, storage, networking, and integration tools that allow systems to work together. IBM Cloud is often used for enterprise and business applications because it focuses on security, reliability, and support for hybrid cloud environments.



Data Flow Diagram (DFD) Description

The Data Flow Diagram illustrates the main interactions between the user, IBM Cloud services, external systems, and internal data stores.

- Initially, the user registers or logs into the system by providing credentials, which are processed by the login function and securely stored in the **User Credentials data store (D1)**. At this stage, the user operates with **lower privileges**, allowing them to view available IBM Cloud services without accessing restricted features.
- When the user chooses to subscribe to a service, they provide payment details that are sent to an external **Bank system**. The bank processes the payment and returns the payment status to the system. Both the bank and its payment data store (**Payment History – D2**) are considered **outside the scope of IBM Cloud**, as payment processing is handled by a third-party entity.
- Once the payment is successfully approved, the user is granted **higher privileges**, enabling access to subscribed services. The user can then use cloud services such as uploading, managing, and viewing files.

- All user data and service-related files are stored in **Cloud Storage (D3)**. Authorized users can retrieve, edit, and manage their stored files through the system, depending on their access level.

Real Life assts and what they do

- **User / Browser**
  Allows users to access IBM Cloud services, view available options, and interact with the system.
- **IBM DataPower Gateway**
  Acts as a gateway that securely connects users and external systems to IBM Cloud services.
- **Web Server & WebSphere Application Server**
  Hosts and runs the main applications that provide IBM Cloud services to users.
- **IBM Cloud Pak for Integration**
  Connects different services and systems together and manages the flow of data between them.
- **Payment Gateway / Payment API**
  Handles payment requests and communicates with the bank to approve or reject transactions.
- **Bank (External System)**
  Processes payments and manages financial transactions outside of IBM Cloud.
- **Cloud Logging and Monitoring**
  Records system activities and helps track usage and system behavior.
- **Object Storage (Cloud Storage)**
  Stores user files and service data so they can be accessed when needed.
- **Virtual Private Cloud (VPC)**
  Provides a private cloud environment where services run in an isolated and controlled space.
- **IBM PureApplication**
  Hosts and manages enterprise applications in a controlled and reliable environment
- **IAM Database**
  Centralized data store that maintains user identities, credentials, roles, permissions, tokens, and policy relationships used to make authentication and authorization decisions across systems.

Risks based on the assets

1."Connector" IBM Cloud Pak: THE DIGITAL NERVOUS SYSTEM

The Business Role

- Ensure that when a customer places an order, the warehouse knows how to ship it, and finance knows how to bill it. It connects to all applications.

The Risk

- Vulnerabilities allow attackers to "cross the wires," stealing sessions or injecting scripts.

BOTTOM LINE: Operational Paralysis. Business units stop communicating; orders fail

2."Engine"WebSphere App Server: The Powerplant

The Business Role

- The heavy-duty engine runs our main websites and mission-critical services.

The Risk

- Java flaws act like "leaving keys in the ignition," allowing full remote-control hijack.

BOTTOM LINE: Total Takeover. Attackers can crash into storefronts or delete essential files.

3."Library" Infosphere: The Source of Truth

The Business Role

- Central Archive for trusted business data, organized for decision-making.

The Risk

- SQL Injection can "poison the well," altering financial figures or deleting databases.

BOTTOM LINE: Data Poisoning. Strategic errors based on false data and GDPR/PCI fines.

4. The "Safe Deposit Box"Cloud VPC: The Secure Vault

The Business Role

- Store critical files, backups, and private workloads.

The Risk

- "Broken locks" allow bypass via skeleton keys. Attackers can break walls, separating data.

BOTTOM LINE: Ransomware. Attackers can encrypt backups, forcing payment.

5. The "Alarm System “Tivoli & Monitoring: The Security Cameras

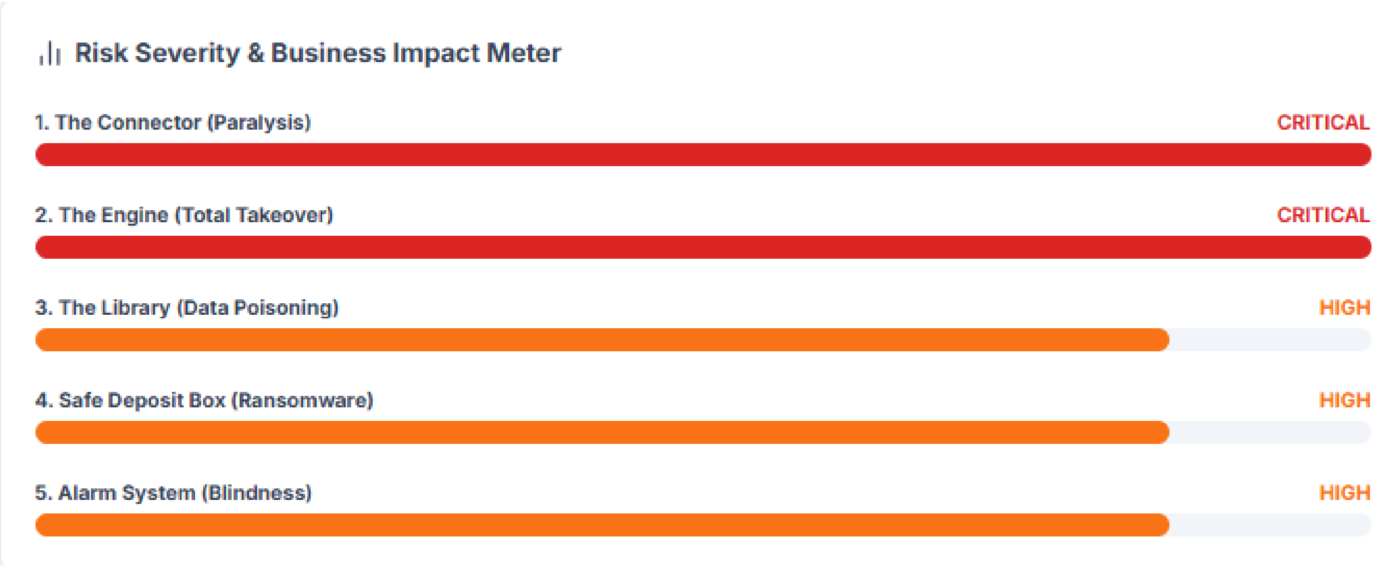
The Business Role

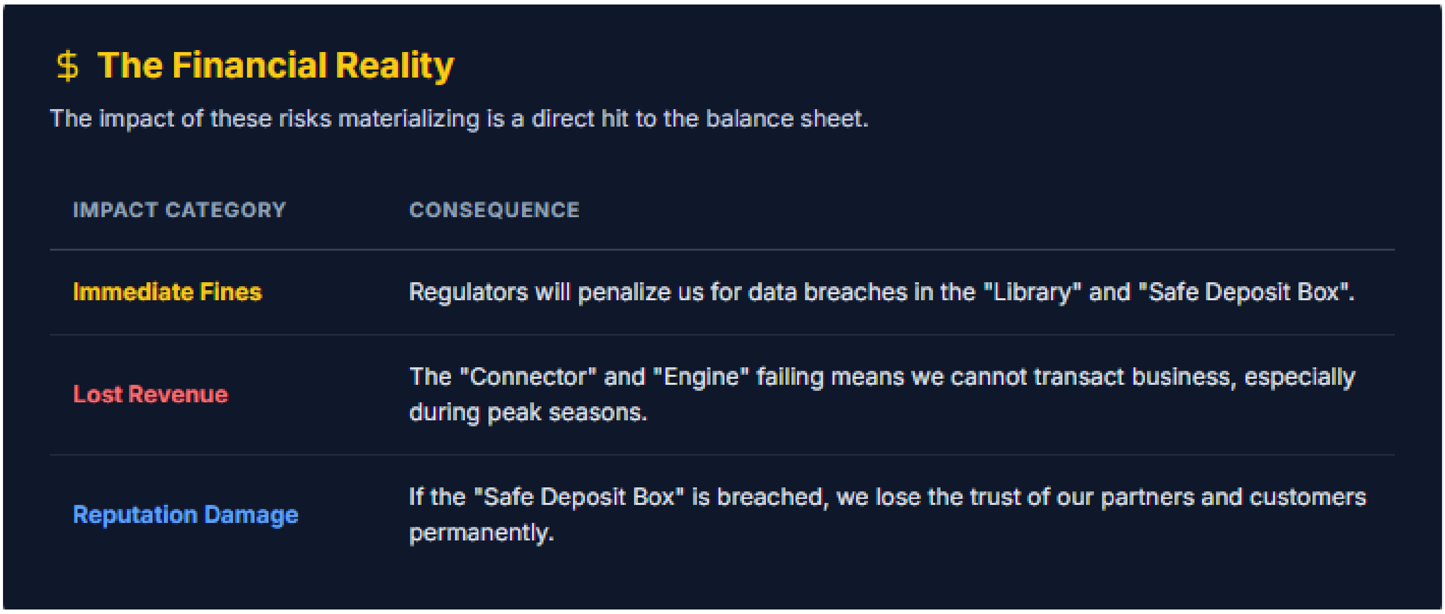
- Watches network 24/7 to detect hackers and provide forensic evidence.

The Risk

- Attackers can turn off alarms or delete logs to hide their tracks.

BOTTOM LINE: Flying Blind. Active attacks (money/data theft) occur without detection.





$ The Financial Reality

The impact of these risks materializing is a direct hit to the balance sheet.

IMPACT CATEGORY	CONSEQUENCE
Immediate Fines	Regulators will penalize us for data breaches in the "Library" and "Safe Deposit Box".
Lost Revenue	The "Connector" and "Engine" failing means we cannot transact business, especially during peak seasons.
Reputation Damage	If the "Safe Deposit Box" is breached, we lose the trust of our partners and customers permanently.

Financial Impact on IBM During Seasonal Peaks

During the holiday season, IBM Cloud Pak for Integration handles a higher volume of data exchanges and transactions because many business processes and customer activities increase. As a result, any attack or outage would affect more transactions, more connected applications, and more users in a shorter period. This amplifies the business impact of disruptions or data exposure, since failures during peak usage can lead to delayed operations, lost revenue, and cascading issues across dependent systems.

Regulatory and Business Risk Context for IBM Cloud Assets

IBM Cloud operates in a highly regulated environment and must comply with global data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations apply whenever personal or sensitive business data is accessed, processed, or stored within IBM Cloud services. Violations can result in severe financial penalties, including fines of up to 4% of annual global revenue under GDPR and up to $7,500 per violation under CCPA, in addition to reputational damage and loss of customer trust.

Based On OSINT Findings

OSINT analysis indicates that IBM Cloud's internet-facing infrastructure is generally well secured, with limited direct exposure. However, credential leakage remains a key risk, as email addresses and passwords may appear in public breach of data or underground sources, particularly through third-party compromises.

Additionally, supply chain and legacy infrastructure risks exist. Historical exposure of SoftLayer-related IP ranges highlights the need for continuous monitoring of acquired or partner environments.

Finally, default credentials represent a critical weakness and must be eliminated through enforced secure configuration baselines and strong identity controls.

OSINT Findings

Target Assessment Report: IBM Cloud

Date: December 10, 2025, **Methodology:** Passive Reconnaissance & Open-Source Intelligence (OSINT)

1. Executive Summary & Strategic Context

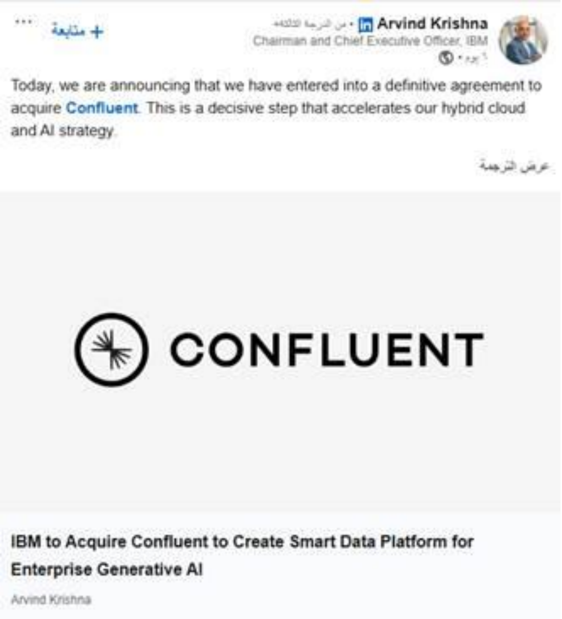
Attack Surface Evolution (2023–2025)

The attack surface of IBM Cloud has expanded significantly due to an inorganic acquisition strategy, introducing new layers of code and potential vulnerabilities.

Timeline of Critical Events:

Date	**Event / Entity**	**Value / Scale**	**Primary Vector / Vulnerability**	**Strategic Implication**
Aug 2023	**Apptio Acquisition**	$4.6B USD	Legacy web footprints; Financial data exposure.	Ingestion of massive datasets (IT Spend) increases data gravity risks. Link
Dec 2023	**StreamSets & webMethods**	**€2.13B EUR**	Data poisoning via complex pipelines; iPaaS surface.	Attack surface extends to the integration layer; "DataOps" risks introduced. Link
2024	**Infrastructure Stress**	*Global*	**Misconfiguration** (Top Linux Threat); Credential saturation.	Cloud credentials commoditized (~$10 on dark web); shift to identity-based attacks. Link
Feb 2025	**HashiCorp Acquisition**	**$6.4B USD**	Secrets Management (Vault); IaC (Terraform).	**Critical Shift:** Third-party Vault risks convert to first-party IBM Cloud liabilities. Link
May 2025	**OT/ICS Surge**	*Sector-wide*	**CVE-2025-32433**; Industrial control targeting.	Operational Technology and IT convergence widens the blast radius. Link
Jun 2025	**Domain Collision**	*Internal*	SoftLayer legacy collisions; NTLM/API leaks.	Technical debt from legacy infrastructure resurfacing as active threats. Link
Aug 2025	**Vault Vulnerability**	*Critical*	**CVE-2025-6014**; TOTP generation code reuse.	Requires immediate patch management; highlights risk of acquired codebases. Link

Dec 2025	**Confluent (Planned)**	*Future*	Kafka Data Streaming.	Anticipated expansion into real-time data movement vectors. **Link**



Arvind Krishna • من الدرجة الثالثة+

Chairman and Chief Executive Officer, IBM

١ يوم •

+ متابعة ···

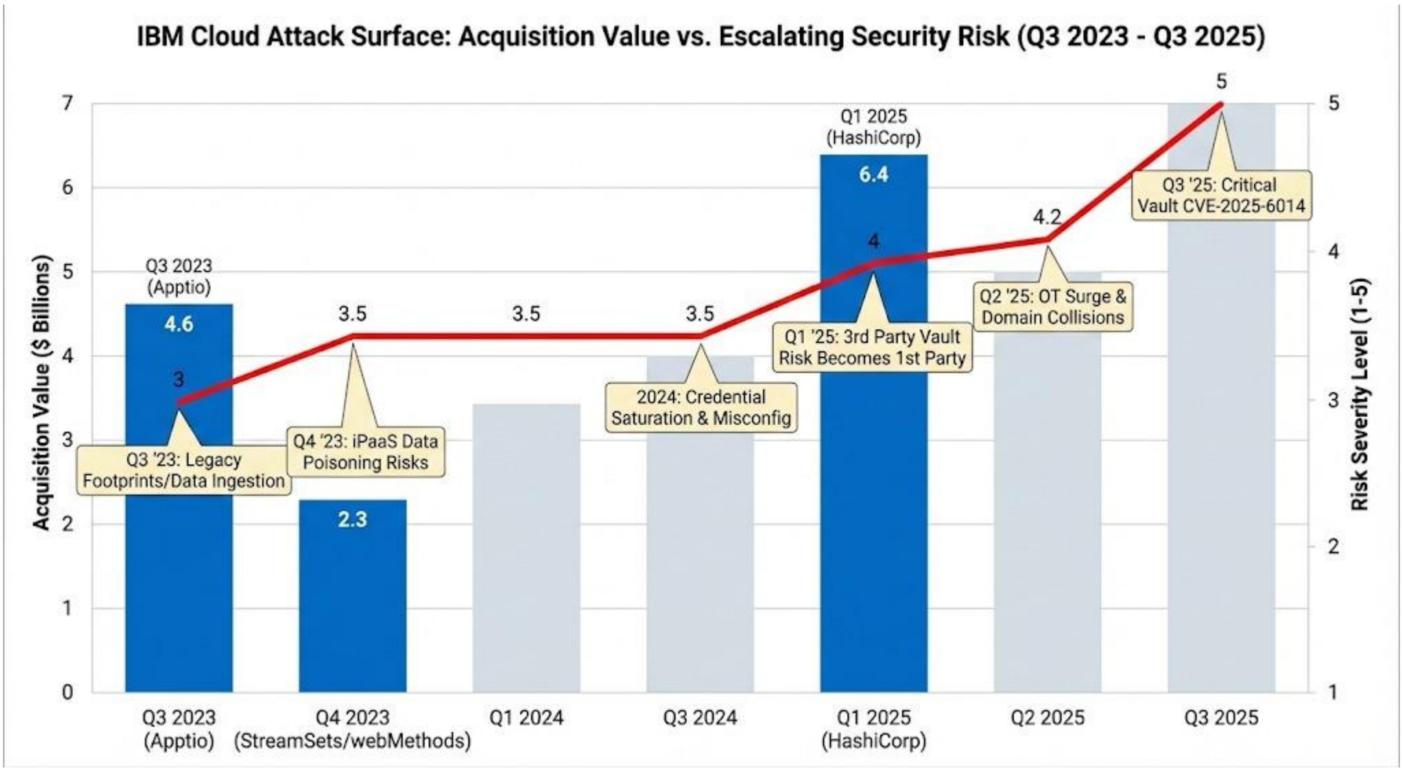
Today, we are announcing that we have entered into a definitive agreement to acquire Confluent. This is a decisive step that accelerates our hybrid cloud and AI strategy.

عرض الترجمة

CONFLUENT

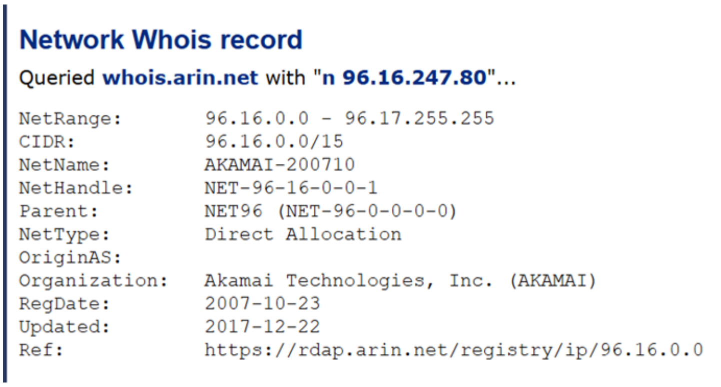
IBM to Acquire Confluent to Create Smart Data Platform for Enterprise Generative AI

Arvind Krishna



IBM Cloud Attack Surface: Acquisition Value vs. Escalating Security Risk (Q3 2023 - Q3 2025)

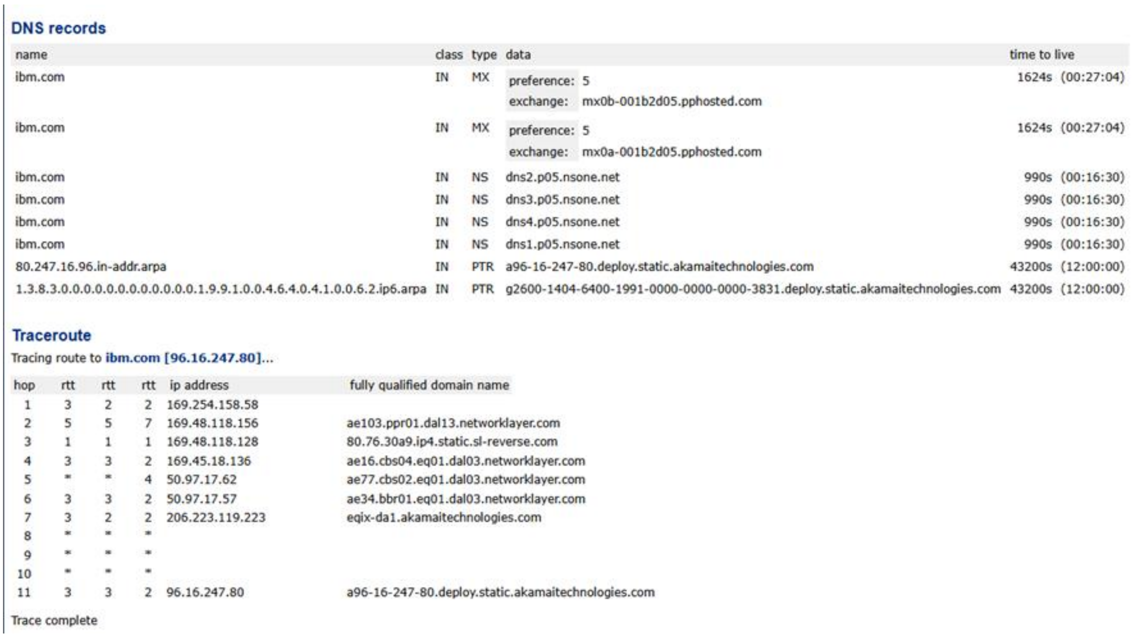
2. Network & Infrastructure Intelligence



Network Whois record

Queried **whois.arin.net** with "**n 96.16.247.80**"...

```
NetRange:       96.16.0.0 - 96.17.255.255
CIDR:           96.16.0.0/15
NetName:        AKAMAI-200710
NetHandle:      NET-96-16-0-0-1
Parent:         NET96 (NET-96-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Akamai Technologies, Inc. (AKAMAI)
RegDate:        2007-10-23
Updated:        2017-12-22
Ref:            https://rdap.arin.net/registry/ip/96.16.0.0
```



DNS records

name	class	type	data	time to live
ibm.com	IN	MX	preference: 5 exchange: mx0b-001b2d05.pphosted.com	1624s (00:27:04)
ibm.com	IN	MX	preference: 5 exchange: mx0a-001b2d05.pphosted.com	1624s (00:27:04)
ibm.com	IN	NS	dns2.p05.nsone.net	990s (00:16:30)
ibm.com	IN	NS	dns3.p05.nsone.net	990s (00:16:30)
ibm.com	IN	NS	dns4.p05.nsone.net	990s (00:16:30)
ibm.com	IN	NS	dns1.p05.nsone.net	990s (00:16:30)
80.247.16.96.in-addr.arpa	IN	PTR	a96-16-247-80.deploy.static.akamaitechnologies.com	43200s (12:00:00)
1.3.8.3.0.0.0.0.0.0.0.0.0.0.0.0.1.9.9.1.0.0.4.6.4.0.4.1.0.0.6.2.ip6.arpa	IN	PTR	g2600-1404-6400-1991-0000-0000-0000-3831.deploy.static.akamaitechnologies.com	43200s (12:00:00)

Traceroute

Tracing route to **ibm.com [96.16.247.80]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	3	2	2	169.254.158.58	
2	5	5	7	169.48.118.156	ae103.ppr01.dal13.networklayer.com
3	1	1	1	169.48.118.128	80.76.30a9.ip4.static.sl-reverse.com
4	3	3	2	169.45.18.136	ae16.cbs04.eq01.dal03.networklayer.com
5	*	*	4	50.97.17.62	ae77.cbs02.eq01.dal03.networklayer.com
6	3	3	2	50.97.17.57	ae34.bbr01.eq01.dal03.networklayer.com
7	3	2	2	206.223.119.223	eqix-da1.akamaitechnologies.com
8	*	*	*		
9	*	*	*		
10	*	*	*		
11	3	3	2	96.16.247.80	a96-16-247-80.deploy.static.akamaitechnologies.com

Trace complete

2.1 Hosting & Legacy Infrastructure

- **CDN / WAF:** Akamai Technologies (AkamaiGHost / AkamaiNetStorage).
- **Legacy Infrastructure:** SoftLayer Technologies (acquired 2013). Legacy configurations, including server naming conventions, remain active within IBM Cloud and contribute to vulnerabilities like unregistered. cloud domains.
- **ASN Information:** AS36351 (IBM Cloud).

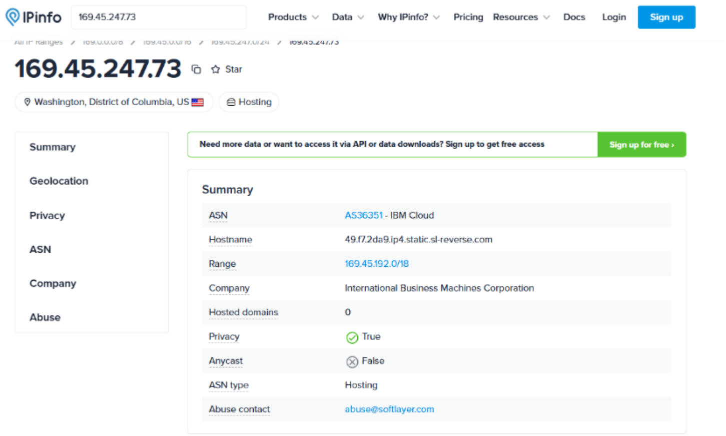
2.2 Web Server Scanning (Nikto Results)

Target: cloud.ibm.com (IP: 23.221.108.76) **Scan Time:** 2025-12-05 11:43:52 (GMT-8)

- **Server Header Leakage:**
  - Server: AkamaiGHost.
  - Uncommon header akamai-grn found.
  - Uncommon header x-reference error found.
  - Server banner changed to AkamaiNetStorage during scanning.

2.3 Identified IP Addresses & Geolocation

- **Active Hosts (Shodan & Network Scan Data):**
  Exposed internal IPs facilitate **SSRF** attacks, which can be used to bypass firewalls or **retrieve sensitive local files** from the server.



169.45.247.73

Washington, District of Columbia, US

Hosting

Need more data or want to access it via API or data downloads? Sign up to get free access

Summary

ASN	AS36351 - IBM Cloud
Hostname	49.f7.2da9.ip4.static.sl-reverse.com
Range	169.45.192.0/18
Company	International Business Machines Corporation
Hosted domains	0
Privacy	✓ True
Anycast	⊗ False
ASN type	Hosting
Abuse contact	abuse@softlayer.com

Link

IP ADDRESS	ASN	DETAILS
169.45.247.73	AS36351 IBM Cloud	0.47ms from Ashburn, US
169.45.192.164	AS36351 IBM Cloud	0.42ms from Ashburn, US
169.45.205.163	AS36351 IBM Cloud	0.43ms from Ashburn, US
169.45.216.51	AS36351 IBM Cloud	0.53ms from Ashburn, US
169.45.246.196	AS36351 IBM Cloud	0.50ms from Ashburn, US
169.45.230.124	AS36351 IBM Cloud	0.50ms from Ashburn, US
169.45.224.20	AS36351 IBM Cloud	0.53ms from Ashburn, US
169.45.222.68	AS36351 IBM Cloud	0.64ms from Ashburn, US
169.45.244.211	AS36351 IBM Cloud	0.58ms from Ashburn, US
169.45.195.68	AS36351 IBM Cloud	0.38ms from Ashburn, US
169.45.231.90	AS36351 IBM Cloud	0.49ms from Ashburn, US
169.45.243.154	AS36351 IBM Cloud	0.42ms from Ashburn, US
169.45.199.156	AS36351 IBM Cloud	0.39ms from Ashburn, US
169.45.206.85	AS36351 IBM Cloud	0.40ms from Ashburn, US
169.45.200.250	AS36351 IBM Cloud	0.55ms from Ashburn, US
169.45.239.156	AS36351 IBM Cloud	0.84ms from Ashburn, US
169.45.193.210	AS36351 IBM Cloud	0.92ms from Ashburn, US
169.45.240.93	AS36351 IBM Cloud	0.39ms from Ashburn, US
169.45.236.114	AS36351 IBM Cloud	0.42ms from Ashburn, US
169.45.217.247	AS36351 IBM Cloud	0.42ms from Ashburn, US
169.45.194.196	AS36351 IBM Cloud	0.40ms from Ashburn, US

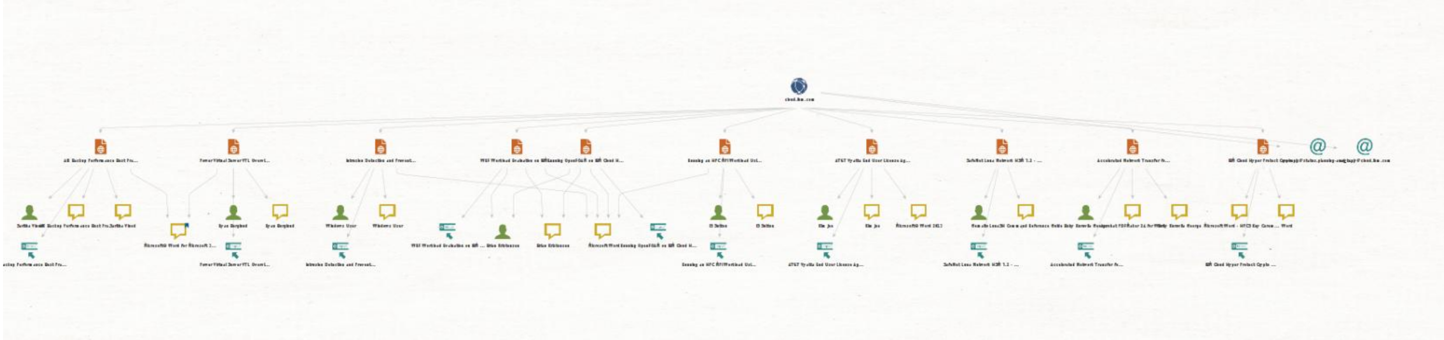
169.45.253.192	AS36351 IBM Cloud	0.38ms from Ashburn, US
169.45.228.122	AS36351 IBM Cloud	0.44ms from Ashburn, US
169.45.226.203	AS36351 IBM Cloud	0.60ms from Ashburn, US
169.45.209.47	AS36351 IBM Cloud	0.42ms from Ashburn, US

2.4 SSL/TLS Configurations

- **Common Certificate Issuer:** DigiCert TLS RSA SHA256 2020 CA1.
- **Common Certificate Subject:** *.us-south.db2w.cloud.ibm.com (Also: *.eu-de.db2w.cloud.ibm.com , *.uk-south.db2w.cloud.ibm.com).
- **Protocols Supported:** TLSv1.2, TLSv1.3.
- **Anomaly:** One host (43.205.255.159) used a self-signed certificate for "Cloud Raxak".

3. Exposed Sensitive Information

3.1 Exposed Technical Documentation



The following PDF documents were identified in public directories, potentially leaking configuration and architecture details:

- PowerVS_AIX_Backup_Performance_Best_Practices_and_Guidelines_v1_0_03012022.pdf
- PowerVS_VTL_Overview.pdf
- IDP_v5.pdf (vSRX)
- HPCC_WRF_workload_report.pdf
- mpi_oneapi_wp_final.pdf
- LunaSH_Command_Reference_Guide_72.pdf (HSM / Crypto)
- accelerated_migration.pdf
- HPCS-Key-Ceremony-using-Key-Part-files.pdf (Critical: Key Ceremony procedures)

3.2 Personnel & Contact Information

Employee Profiles (LinkedIn):

- (15) Arvind Krishna | LinkedIn à CEO of IBM
- (15) Jayendra Pawar | LinkedIn à Backend Engineer @IBM
- (15) Pratiksha Anand | LinkedIn à Backend Developer @IBM Cloud(ISDL)
- (15) Aleksandar Nikolov | LinkedIn à Cloud Operations Engineer at IBM
- (15) Deepankar Mohanty | LinkedIn à Senior Network Engineer at SoftLayer(IBM Cloud
- (14) Ahmed Magdy Foda | LinkedIn à Cyber Security Consultant at IBM

Identified Email Addresses:

- **Service/Admin:** dnsadm@us.ibm.com, webmaste@us.ibm.com , imadmin@us.ibm.com, admin@in.ibm.com, redbooks@us.ibm.com, IBM.India.Grievance.Officer@ibm.com, blueline@be.ibm.com, uaserv@ua.ibm.com, infoibm@us.ibm.com, ibmidsupportuk@ibm.com.
- **Internal/Employee:** maximona@us.ibm.com, llmater@us.ibm.com, jinho@us.ibm.com, srilatta@us.ibm.com, twlawrie@us.ibm.com, sadanand.shastri@us.ibm.com, lsracf2@us.ibm.com, mayp@us.ibm.com , cstrain@us.ibm.com.
- **Automated:** no-reply@status.planning-analytics.cloud.ibm.com, no_reply@cloud.ibm.com.

à These emails can be used for phishing.

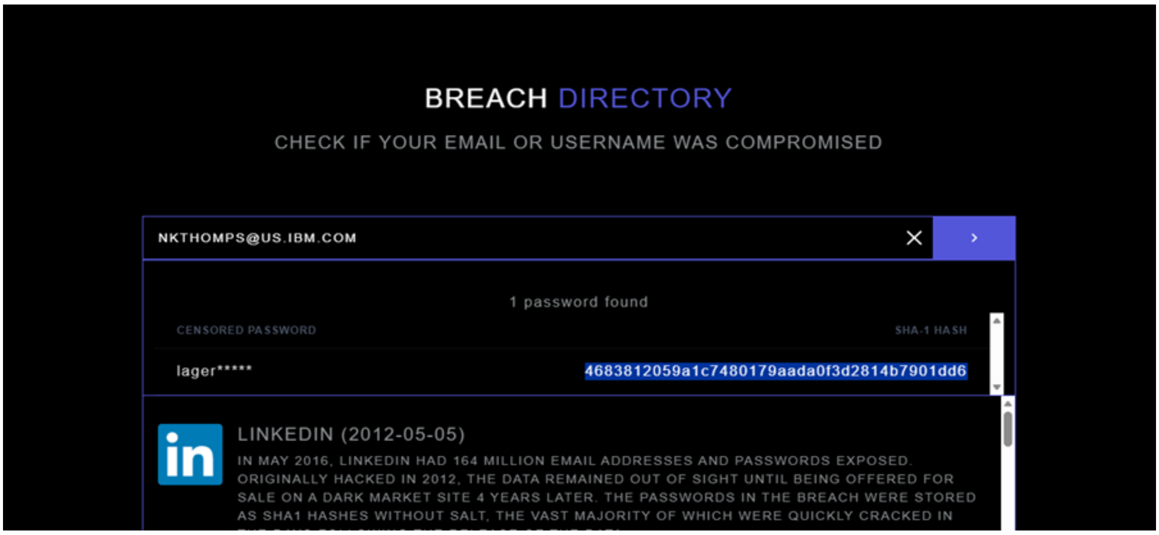
4. Identity & Access Management (IAM) Intelligence

4.1 Compromised / Leaked Credentials

dnsadm@us.ibm.com à WvTdQx

webmaste@us.ibm.com à possible passwords: (33865889e5, d3481ae553, e5fb0b05fd, f78688fb6a)

nkthomps@us.ibm.com à lager1tat
massing@us.ibm.com à Jetski129



BREACH DIRECTORY

CHECK IF YOUR EMAIL OR USERNAME WAS COMPROMISED

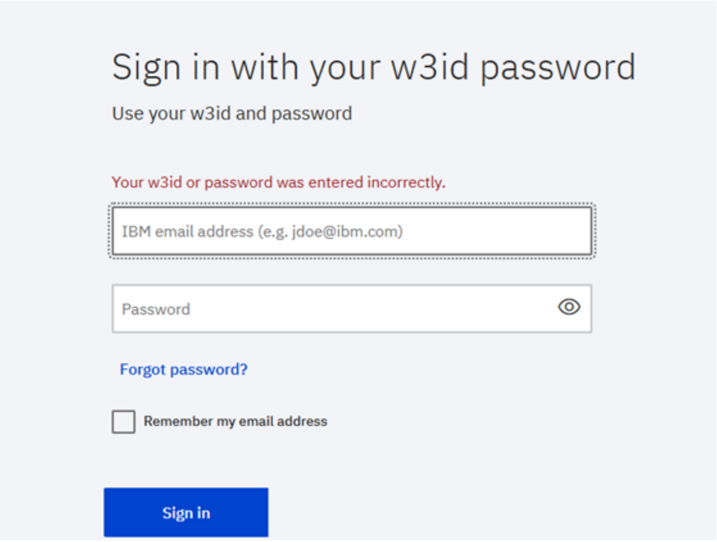
NKTHOMPS@US.IBM.COM

1 password found

CENSORED PASSWORD	SHA-1 HASH
lager*****	4683812059a1c7480179aada0f3d2814b7901dd6

LINKEDIN (2012-05-05)

IN MAY 2016, LINKEDIN HAD 164 MILLION EMAIL ADDRESSES AND PASSWORDS EXPOSED. ORIGINALLY HACKED IN 2012, THE DATA REMAINED OUT OF SIGHT UNTIL BEING OFFERED FOR SALE ON A DARK MARKET SITE 4 YEARS LATER. THE PASSWORDS IN THE BREACH WERE STORED AS SHA1 HASHES WITHOUT SALT, THE VAST MAJORITY OF WHICH WERE QUICKLY CRACKED IN



Sign in with your w3id password

Use your w3id and password

Your w3id or password was entered incorrectly.

IBM email address (e.g. jdoe@ibm.com)

Password

Forgot password?

□ Remember my email address

Sign in

We tried all the passwords, but none of them were valid.

We can use this to figure out the password pattern and perform a brute-force attack.

4.2 Default Credentials Reference:

Default credentials can be exploited in subsequent attacks if they are left unchanged due to oversight.

Product	Version	Access Method	Username	Default Password	Impact	Notes
IBM 2210			**def**	**trade**		RIP
IBM 3534 F08 Fibre Switch		Multi	**admin**	**password**	Admin	
IBM 3583 Tape Library		HTTP	**admin**	**secure**	Admin	
IBM 390e		Multi	**n/a**	**admin**	Admin	
IBM 600x		Multi	**n/a**	**admin**	Admin	
IBM 8224 HUB		Multi	**vt100**	**public**	Admin	Swap MAC address chip from other 8224
IBM 8225		Multi	**I5rDv2b2JjA8Mm**	**A52896nG93096a**	Admin	
IBM 8237		Multi	**I5rDv2b2JjA8Mm**	**A52896nG93096a**	Admin	
IBM 8239 Token Ring HUB	2.5	Console	**n/a**	**R1QTPS**	Utility Program	
IBM a20m		Multi	**n/a**	**admin**	Admin	
IBM A21m		Multi	**n/a**	**(none)**	Admin	
IBM AIX		Multi	**guest**	**(none)**	User	
IBM AIX		Multi	**guest**	**guest**	User	
IBM AIX	4.X	Multi	**admin**	**admin**	User	
IBM Aptiva			**n/a**	**n/a**	CMOS	Press both mouse buttons repeatedly during boot to bypass CMOS password
IBM AS/400			**qpgmr**	**qpgmr**		
IBM AS/400			**QSECOFR**	**QSECOFR**		Any

IBM AS/400			**QSRV**	**QSRV**		
IBM AS/400			**QSRVBAS**	**QSRVBAS**		
IBM AS/400			**qsysopr**	**qsysopr**		
IBM AS/400			**QUSER**	**QUSER**		OS/400
IBM Ascend OEM Routers		Telnet	**n/a**	**ascend**	Admin	
IBM Bladecenter Advanced Management Module			**USERID**	**PASSW0RD**		Added: *2016-10-31*
IBM BladeCenter Mgmt Console		HTTP	**USERID**	**PASSW0RD**	Admin	
IBM CICS			**$SRV**	**$SRV**		
IBM CICS			**CICSUSER**	**CISSUS**		
IBM CICS			**DBDCCICS**	**DBDCCIC**		
IBM CICS			**FORSE**	**FORSE**		
IBM CICS			**OPER**	**OPER**		
IBM CICS			**POST**	**BASE**		
IBM CICS			**PRODCICS**	**PRODCICS**		
IBM CICS			**PROG**	**PROG**		
IBM CICS			**SYSA**	**SYSA**		
IBM CICS			**VCSRV**	**VCSRV**		
IBM DB2			**db2admin**	**db2admin**		WinNT
IBM DB2			**db2fenc1**	**db2fenc1**		
IBM DB2			**db2inst1**	**db2inst1**		Added: *2016-10-31*

IBM Directory - Web Administration Tool	5.1	HTTP	**superadmin**	**secret**	Admin	Documented in Web Administration Guide
IBM Domino Go			**webadmin**	**webibm**		Added: *2016-10-31*
IBM Hardware Management Console	3	ssh	**hscroot**	**abc123**	Admin	
IBM HMC			**hscroot**	**abc123**		Added: *2016-10-31*
IBM HMC			**root**	**passw0rd**		Added: *2016-10-31*
IBM IBM		Multi	**n/a**	**(none)**	Admin	
IBM Infoprint 6700		Multi	**root**	**(none)**	Admin	Also works for older 4400 printers and probably Printronics equivalents as well.
IBM Information Archive Appliance			**iscadmin**	**iscadmin**	Information Archive Admin interface	Added: *2012-01-08*
IBM Information Archive Appliance		Cluster node servers	**root**	**i8root**	Root access	Added: *2012-01-08*
IBM Information Archive Appliance		IBM Remote Support Manager for Storage server	**admin**	**rsm33inst**	Admin Access	Added: *2012-01-08*
IBM Information Archive Appliance		IBM Remote Support Manager for Storage server	**lservice**	**rsm33inst**	Service Access	Added: *2012-01-08*

IBM Information Archive Appliance		IBM Remote Support Manager for Storage server	**root**	**rsm33inst**	Root Access	Added: *2012-01-08*
IBM Information Archive Appliance		KVM Console	**(none)**	**(blank)**	Access to the KVM Console	No password by default; if you find it password protected we can't help Added: *2012-01-08*
IBM Information Archive Appliance		Management console server	**iaadmin**	**iaadmin**	Install upgrades and the IBM Systems Director interface	Added: *2012-01-08*
IBM Information Archive Appliance		Management console server	**root**	**i8root**	Root access	Added: *2012-01-08*
IBM Integrated Management Module (IMM)			**USERID**	**PASSW0RD**		Added: *2016-10-31*
IBM LAN Server / OS/2			**username**	**password**		2.1 3.0 4.
IBM Lotus Domino Go WebServer (net.commerce edition)			**webadmin**	**webibm**		ANY ?
IBM management hw		Multi	**USERID**	**PASSW0RD**	admin	
IBM NetCommerce PRO			**ncadmin**	**ncadmin**		3.2
IBM OS/400			**QSECOFR**	**QSECOFR**		OS/400
IBM OS/400		Multi	**11111111**	**11111111**		
IBM OS/400		Multi	**22222222**	**22222222**		
IBM OS/400		Multi	**ibm**	**2222**		
IBM OS/400		Multi	**ibm**	**password**		

IBM OS/400		Multi	**ibm**	**service**		
IBM OS/400		Multi	**qpgmr**	**qpgmr**		
IBM OS/400		Multi	**qsecofr**	**11111111**		
IBM OS/400		Multi	**qsecofr**	**22222222**		
IBM OS/400		Multi	**qsecofr**	**qsecofr**		
IBM OS/400		Multi	**qserv**	**qserv**		
IBM OS/400		Multi	**qsrv**	**11111111**		
IBM OS/400		Multi	**qsrv**	**22222222**		
IBM OS/400		Multi	**qsrv**	**qsrv**		
IBM OS/400		Multi	**qsrvbas**	**qsrvbas**		
IBM OS/400		Multi	**qsvr**	**ibmcel**		
IBM OS/400		Multi	**qsvr**	**qsvr**		
IBM OS/400		Multi	**qsysopr**	**qsysopr**		
IBM OS/400		Multi	**quser**	**quser**		
IBM OS/400		Multi	**secofr**	**secofr**		
IBM OS/400		Multi	**sedacm**	**sedacm**		
IBM OS/400		Multi	**sysopr**	**sysopr**		
IBM OS/400		Multi	**userp**	**(none)**	No	
IBM PC BIOS		Console	**n/a**	**IBM**	Admin	
IBM PC BIOS		Console	**n/a**	**MBIU0**	Admin	
IBM PC BIOS		Console	**n/a**	**merlin**	No	
IBM PC BIOS		Console	**n/a**	**sertafu**	Admin	
IBM POS CMOS		Console	**ESSEX**			
IBM POS CMOS		Console	**IPC**			
IBM RACF			**IBMUSER**	**SYS1**		

IBM Remote Supervisor Adapter (RSA)		HTTP	**USERID**	**PASSW0RD**	Admin	
IBM RS/6000			**root**	**ibm**		AIX
IBM RSA	5	HTTP	**wpsadmin**	**wpsadmin**	9091	
IBM SONAS			**USERID**	**PASSWORD**		Added: *2016-10-31*
IBM Sterling Managed File Transfer			**fg_sysadmin**	**password**		Added: *2016-10-31*
IBM switch	8275-217	Telnet	**admin**	**(none)**	Admin	
IBM T20		Multi	**n/a**	**admin**	Admin	
IBM T42		HTTP	**Administrator**	**admin**	Admin	
IBM Tivoli		HTTP	**admin**	**admin**	Admin	
IBM TotalStorage Enterprise Server		Multi	**storwatch**	**specialist**	Admin	
IBM TS3100(3573-L2U)		http	**admin**	**secure**		
IBM TS4300		GUI	**administrator**	**adm001**	administrator	Added: *2024-04-25*
IBM VM/CMS		Multi	**$ALOC$**	**(none)**		
IBM VM/CMS		Multi	**ADMIN**	**(none)**		
IBM VM/CMS		Multi	**AP2SVP**	**(none)**		
IBM VM/CMS		Multi	**APL2PP**	**(none)**		
IBM VM/CMS		Multi	**AUTOLOG1**	**(none)**		
IBM VM/CMS		Multi	**BATCH**	**(none)**		
IBM VM/CMS		Multi	**BATCH1**	**(none)**		
IBM VM/CMS		Multi	**BATCH2**	**(none)**		

IBM VM/CMS		Multi	**CCC**	**(none)**		
IBM VM/CMS		Multi	**CMSBATCH**	**(none)**		
IBM VM/CMS		Multi	**CMSBATCH**	**CMSBATCH**		
IBM VM/CMS		Multi	**CMSUSER**	**(none)**		
IBM VM/CMS		Multi	**CPNUC**	**(none)**		
IBM VM/CMS		Multi	**CPRM**	**(none)**		
IBM VM/CMS		Multi	**CSPUSER**	**(none)**		
IBM VM/CMS		Multi	**CVIEW**	**(none)**		
IBM VM/CMS		Multi	**DATAMOVE**	**(none)**		
IBM VM/CMS		Multi	**DEMO1**	**(none)**		
IBM VM/CMS		Multi	**DEMO2**	**(none)**		
IBM VM/CMS		Multi	**DEMO3**	**(none)**		
IBM VM/CMS		Multi	**DEMO4**	**(none)**		
IBM VM/CMS		Multi	**DIRECT**	**(none)**		
IBM VM/CMS		Multi	**DIRMAINT**	**(none)**		
IBM VM/CMS		Multi	**DISKCNT**	**(none)**		
IBM VM/CMS		Multi	**EREP**	**(none)**		
IBM VM/CMS		Multi	**FSFADMIN**	**(none)**		
IBM VM/CMS		Multi	**FSFTASK1**	**(none)**		
IBM VM/CMS		Multi	**FSFTASK2**	**(none)**		
IBM VM/CMS		Multi	**GCS**	**(none)**		
IBM VM/CMS		Multi	**IDMS**	**(none)**		
IBM VM/CMS		Multi	**IDMSSE**	**(none)**		
IBM VM/CMS		Multi	**IIPS**	**(none)**		
IBM VM/CMS		Multi	**IPFSERV**	**(none)**		

IBM VM/CMS		Multi	**ISPVM**	**(none)**		
IBM VM/CMS		Multi	**IVPM1**	**(none)**		
IBM VM/CMS		Multi	**IVPM2**	**(none)**		
IBM VM/CMS		Multi	**MAINT**	**(none)**		
IBM VM/CMS		Multi	**MAINT**	**MAINT**		
IBM VM/CMS		Multi	**MOESERV**	**(none)**		
IBM VM/CMS		Multi	**NEVIEW**	**(none)**		
IBM VM/CMS		Multi	**OLTSEP**	**(none)**		
IBM VM/CMS		Multi	**OP1**	**(none)**		
IBM VM/CMS		Multi	**OPERATNS**	**(none)**		
IBM VM/CMS		Multi	**OPERATNS**	**OPERATNS**		
IBM VM/CMS		Multi	**OPERATOR**	**(none)**		
IBM VM/CMS		Multi	**OPERATOR**	**OPERATOR**		
IBM VM/CMS		Multi	**PDMREMI**	**(none)**		
IBM VM/CMS		Multi	**PENG**	**(none)**		
IBM VM/CMS		Multi	**PROCAL**	**(none)**		
IBM VM/CMS		Multi	**PRODBM**	**(none)**		
IBM VM/CMS		Multi	**PROMAIL**	**(none)**		
IBM VM/CMS		Multi	**PSFMAINT**	**(none)**		
IBM VM/CMS		Multi	**PVM**	**(none)**		
IBM VM/CMS		Multi	**RDM470**	**(none)**		
IBM VM/CMS		Multi	**ROUTER**	**(none)**		
IBM VM/CMS		Multi	**RSCS**	**(none)**		
IBM VM/CMS		Multi	**RSCSV2**	**(none)**		
IBM VM/CMS		Multi	**SAVSYS**	**(none)**		

IBM VM/CMS		Multi	**SFCMI**	**(none)**		
IBM VM/CMS		Multi	**SFCNTRL**	**(none)**		
IBM VM/CMS		Multi	**SMART**	**(none)**		
IBM VM/CMS		Multi	**SQLDBA**	**(none)**		
IBM VM/CMS		Multi	**SQLUSER**	**(none)**		
IBM VM/CMS		Multi	**SYSADMIN**	**(none)**		
IBM VM/CMS		Multi	**SYSCKP**	**(none)**		
IBM VM/CMS		Multi	**SYSDUMP1**	**(none)**		
IBM VM/CMS		Multi	**SYSERR**	**(none)**		
IBM VM/CMS		Multi	**SYSWRM**	**(none)**		
IBM VM/CMS		Multi	**TDISK**	**(none)**		
IBM VM/CMS		Multi	**TEMP**	**(none)**		
IBM VM/CMS		Multi	**TSAFVM**	**(none)**		
IBM VM/CMS		Multi	**VASTEST**	**(none)**		
IBM VM/CMS		Multi	**VM3812**	**(none)**		
IBM VM/CMS		Multi	**VMARCH**	**(none)**		
IBM VM/CMS		Multi	**VMASMON**	**(none)**		
IBM VM/CMS		Multi	**VMASSYS**	**(none)**		
IBM VM/CMS		Multi	**VMBACKUP**	**(none)**		
IBM VM/CMS		Multi	**VMBSYSAD**	**(none)**		
IBM VM/CMS		Multi	**VMMAP**	**(none)**		
IBM VM/CMS		Multi	**VMTAPE**	**(none)**		
IBM VM/CMS		Multi	**VMTLIBR**	**(none)**		
IBM VM/CMS		Multi	**VMUTIL**	**(none)**		
IBM VM/CMS		Multi	**VSEIPO**	**(none)**		

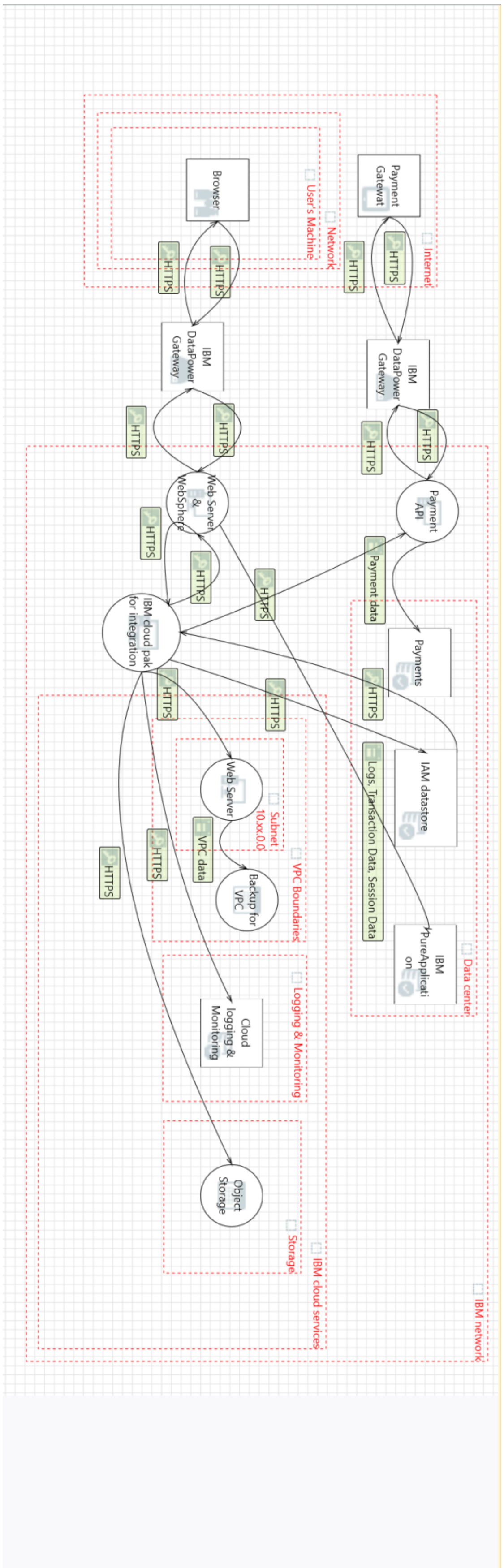
IBM VM/CMS		Multi	**VSEMAINT**	**(none)**		
IBM VM/CMS		Multi	**VSEMAN**	**(none)**		
IBM VM/CMS		Multi	**VTAM**	**(none)**		
IBM VM/CMS		Multi	**VTAM**	**VTAM**		
IBM VM/CMS		Multi	**VTAMUSER**	**(none)**		

5. Publicly available code repositories:

Link: https://github.com/IBM-Cloud
https://github.com/IBM/cloud-pak
https://github.com/IBM/ibm-pak

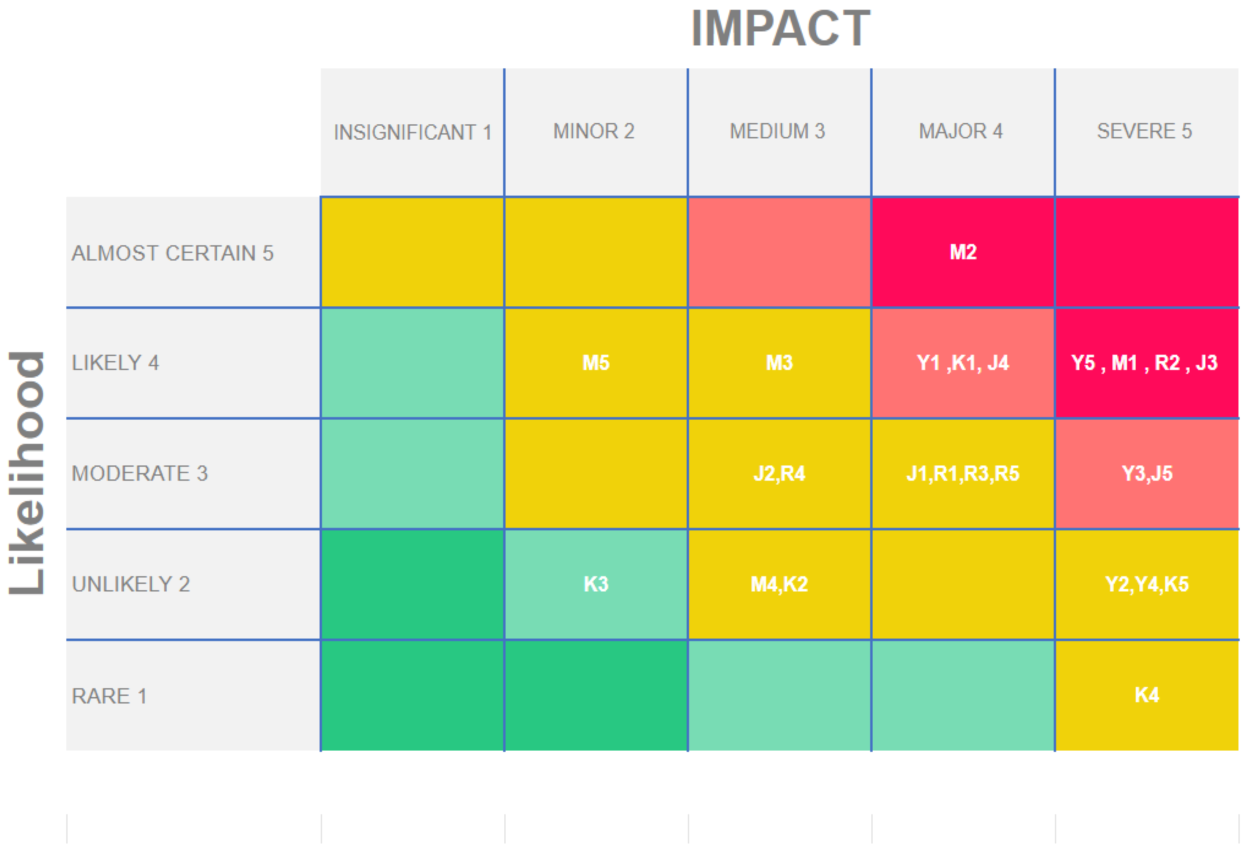
Risk: Exposes IBM Cloud infrastructure allowing malicious users to craft tailored attacks.

Technical Data Flow Diagram (DFD) Description



Real Life assts and their Threats

Heat Map



IMPACT

Likelihood	INSIGNIFICANT 1	MINOR 2	MEDIUM 3	MAJOR 4	SEVERE 5
ALMOST CERTAIN 5				M2	
LIKELY 4		M5	M3	Y1 ,K1, J4	Y5 , M1 , R2 , J3
MODERATE 3			J2,R4	J1,R1,R3,R5	Y3,J5
UNLIKELY 2		K3	M4,K2		Y2,Y4,K5
RARE 1					K4

M1- Security Bulletin: IBM Cloud Pak System is vulnerable to an Improper Access Control due to use of Apache Commons BeanUtils [CVE-2025-48734]

Asset: IBM Cloud Pak System

Vulnerability: Improper Access Control lead to RCE

Initial Access:
The attacker starts with a **low-privileged account** and sends crafted input that reaches PropertyUtilsBean.getProperty() in Apache Commons BeanUtils.

Exploitation:
The unsafe property access exposes the application's **ClassLoader** à allowing the attacker to load malicious classes or inject arbitrary bytecode.

Remote Code Execution:
By controlling the ClassLoader, the attacker executes arbitrary code inside the JVM, gaining full control of the application's runtime.

Privilege Escalation:

The malicious code runs with the same privileges as the JVM process.
If the service account has elevated OS or platform permissions à the attacker can escalate further and compromise the entire system (Lateral Movement).

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

STRIDE:

Tampering: The attacker can tamper with the application's runtime by loading malicious classes through the ClassLoader and altering the system's behavior.

Repudiation: If the application does not log property access or class-loading events, the attacker can perform the attack without leaving any trace.

Information Disclosure: The attacker can access internal class metadata through the declaredClass property and this leading to information disclosure about the application's classes and class-loading environment.

Denial of Service: The attacker can cause a denial of service by loading malicious or unstable classes through the ClassLoader and potentially crashing the JVM.

Elevation of Privilege: The attacker can achieve elevation of privilege by executing arbitrary code with the same permissions as the application's JVM process.

Likelihood: 4 / 5

The vulnerability is easy to exploit because it has Low Attack Complexity.
It requires Low Privileges, meaning the attacker only needs a basic authenticated account.
It requires no user interaction.

Impact: 5 / 5

The vulnerability allows full RCE in the JVM and gives the attacker complete control over the system.

Risk = 4 × 5 = 20 / 25 à Very High Risk

Damage (9/10): Allows full RCE inside the JVM with complete compromise of C/I/A.

Reproducibility (8/10): The exploit is consistently repeatable via the same vulnerable property-access path.

Exploitability (8/10): Low complexity and low privileges make the attack easy to perform.

Affected Users (8/10): Any Cloud Pak service using the vulnerable BeanUtils code is exposed.

Discoverability (7/10): The flaw is findable by analyzing property access in a widely known library.

Final DREAD Score: 40/50

M2 - https://www.ibm.com/support/pages/node/7162199

Asset: IBM Watson Speech Services Cartridge (add-on) for IBM Cloud Pak for Data

Vulnerability: path traversal in onnx

Initial Access:

The attacker sends an unauthenticated request with ../ to the exposed ONNX endpoint.

Exploitation:

The payload bypasses validation and performs directory traversal on the filesystem.

Information Disclosure:

The attacker reads sensitive files such as configs, credentials or logs.

Privilege Escalation (Potential):

Stolen credentials or keys may let the attacker gain higher-privileged access.

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

STRIDE:

Information Disclosure: Reading arbitrary files on the system, exposing sensitive information such as configuration files, credentials, or model data.

DoS: Accessing large system files through path traversal can trigger errors or consume excessive resources, and repeated reads on the same file or directory can create recursive processing loops that overwhelm the service and cause it to crash.

Elevation of Privilege: may reading configuration or credential files may allow an attacker to later escalate privileges à such as stealing keys or login data.

Likelihood: 5/5

Attack Vector: Network
The attack can be launched remotely over the network à without physical access or local presence.
Attack Complexity: Low
Exploitation is straightforward and does not require special conditions**.**

Privileges Required: None
The attacker does not need to be authenticated or high privileges.

User Interaction: None
The attack does not depend on any action from a user to succeed.

Impact: 4/5

Sensitive system files could be exposed

Risk = 5 × 4 = 20 / 25 à Very High Risk

Damage: 8/10

Sensitive file disclosure à possible indirect privilege escalation.

Reproducibility: 10/10

Works every time with a simple ../ request.

Exploitability: 10/10

Unauthenticated, remote and trivial payload.

Affected Users: 8/10

Compromises the system’s files and any component using exposed credentials.

Discoverability: 10/10

Endpoint and flaw are obvious once exposed.

Total: 46/50

M3 - Security Bulletin: WebSphere Application Server Edge Caching Proxy may be vulnerable to HTTP response splitting (CVE-2017-1503)

Asset: WebSphere

Vulnerability: WebSphere Application Server Edge Caching Proxy may be vulnerable to HTTP response splitting

Initial Access: Attacker sends a crafted HTTP request with \r\n to the Edge Caching Proxy.

Exploitation: Server fails to validate input, splitting the response and injecting headers or content.

Privilege Escalation: The XSS that could result from this vulnerability may lead to higher privileged accounts

CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

STRIDE:

Tampering

Attacker injects malicious headers and modifies the server's HTTP response

Information Disclosure

Split responses may expose sensitive data returned by the server

Likelihood: 4/5

The attack is remote, requires no privileges, has low complexity and only needs user interaction to clicke URL.

Impact: 3/5

The attacker can inject headers and content, enabling cache poisoning, XSS and limited information disclosure.

Risk = 3 * 5 = 15 / 25 à Medium

Damage (6/10):

Enables cache poisoning, XSS and limited data exposure à no RCE or privilege escalation.

Reproducibility (9/10):

Highly repeatable using the same crafted payload.

Exploitability (8/10):

Low complexity, no privileges required, only user click needed.

Affected Users (5/10):

Impact varies depending on which cached pages or users are served poisoned responses.

Discoverability (7/10):

Header manipulation issues are relatively easy to identify and test for.

Total: 35 / 50 → Medium Risk.

M4 - Security Bulletin: IBM DataPower Gateway vulnerability in TLS (CVE-2020-4831)

Asset: IBM DataPower Gateway

Vulnerability:

IBM DataPower Gateway uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.

Initial Access: The attacker connects to the exposed TLS endpoint on the DataPower Gateway.

Exploitation: They exploit weak or outdated cryptographic algorithms during the TLS handshake.

Data Exposure: The attacker passively captures encrypted traffic and uses cryptographic weaknesses to decrypt sensitive information.

Lateral Movement: It is possible that he could find a way to move from one device to another after Knowing the encryption method and the information.

Post-Exploitation:
Decrypted data à credentials or tokens, may be used for further attacks.

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

STRIDE:

Information Disclosure: An attacker may decrypt sensitive information.

Likelihood: 2/5

The attack is remote, requires no privileges and no user interaction à but it has high complexity, making exploitation moderately difficult.

Impact: 3/5

The vulnerability allows exposure of highly sensitive information.

Risk = 3 * 3 = 6 à Low

Damage (7/10):
Decryption of highly sensitive data.

Reproducibility (4/10):
Complex cryptographic attack; not easily repeated without advanced capability.

Exploitability (3/10):
High attack complexity makes exploitation difficult.

Affected Users (5/10):
Any user relying on the gateway for encrypted communications may be exposed.

Discoverability (4/10):
Weak crypto is not trivial to detect without deep inspection or cryptanalysis expertise.

Total: 23 / 50 → Low Risk

M5 - Security Bulletin: Log viewer vulnerability affects IBM PureApplication System (CVE-2014-6190)

Asset: IBM PureApplication System

Vulnerability: **Information Disclosure allow access Log viewer**

Initial Access:
The attacker sends a direct HTTP request to the log viewer URL exposed by the PureApplication System.

Exploitation:
Because access controls are missing, the system returns log viewer pages to an unauthorized user.

Information Disclosure:
The attacker reads sensitive log data such as system messages, stack traces, usernames or internal paths.

Post-Exploitation:
Exposed log data can help the attacker map the system, identify components or gather info for later attacks.

CVSS Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Repudiation: Attacker may find a way to change log files.

Information Disclosure: Unauthorized users can access log pages and view sensitive information.

Likelihood: 4/5

Because attackers just access a known URL and require no privileges or special conditions.

Impact: 2/5

Only logs are exposed, without affecting integrity or availability

Total Risk = 4 * 2 = 8 → Low

Damage: 2/10

Only log data exposed à no integrity or availability impact.

Reproducibility: 10/10

Just enter a URL.

Exploitability: 9/10

No auth, low complexity, fully remote.

Affected Users: 3/10

Data exposure limited to logs only.

Discoverability: 10/10

URL patterns are predictable and easy to guess.

Total: 34 / 50 → Low Risk

Threat Propagation Matrix

Vulnerability / Asset	Entry Point	Primary Impact	Propagation Path	Final Impact
1. Cloud Pak System – BeanUtils RCE	Authenticated user with low Privilege	Full JVM RCE	Malicious code executes → steals service creds → pivot to filesystem, DB, or internal APIs	Full system compromise, lateral movement, privilege escalation across Cloud Pak components
2. Watson Speech Services – ONNX Path Traversal	Public ONNX endpoint	File disclosure	Reads config/credential files → attacker obtains API keys or tokens	Unauthorized access to Cloud Pak for Data services, impersonation, further privilege escalation
3. WebSphere Edge Caching Proxy – Response Splitting	Edge proxy HTTP endpoint	Cache poisoning, injected headers	Poisoned cache affects downstream clients → users receive malicious responses	XSS, session token theft, tricking internal users, spreading malicious payloads through cached pages
4. DataPower Gateway – Weak TLS	External TLS interface	Decrypted traffic (passive)	Attacker extracts credentials/tokens from decrypted sessions	Unauthorized access to backend services, takeover of API calls, replay attacks
5. PureApplication System – Log Viewer Exposure	Direct URL access (no auth)	Log data disclosure	Leaked logs reveal endpoints, stack traces, usernames → attacker maps system	Targeted attacks on identified services, easier exploitation of other weaknesses

Contextual Risk Register

Risk Event	**Context (Asset/Process)**	**Business Impact**	**Real Score**
Improper Access Control (RCE)	**IBM Cloud Pak System** **Hosts the entire hybrid cloud infrastructure, including virtual machines and containerized applications.**	**Attackers gain full control of the application runtime (JVM). Potential for total system compromise and lateral movement.**	**Very High**
Path Traversal **(ONNX Endpoint)**	**IBM Watson Speech Services** • **Powers automated customer interactions like virtual assistants and real-time call transcription.** • **Processes sensitive PII, including raw voice recordings and financial or personal details mentioned during calls.**	**Exposure of critical configuration files and credentials (API keys). Potential service crash (DoS) due to recursive loops.**	**Very High**

HTTP Response Splitting	**WebSphere Edge Caching Proxy** · Serves as the front-end delivery point to cache web content and optimize performance for end-users. · Handles temporary user session data and cached web pages, acting as the public face of the application.	Risk of Web Cache Poisoning and XSS. Users may be served malicious content, though the server itself is not breached.	Medium
Weak TLS Cryptography	**IBM DataPower Gateway** · Acts as the security gatekeeper for all API traffic and mobile/B2B integrations. · Processes high-value transaction data	Highly sensitive encrypted traffic can be decrypted by attackers, exposing credentials or tokens.	Low
Information Disclosure	**IBM PureApplication System** • Stores system configurations, internal architecture maps, and operational logs that contain sensitive network details.	Unauthorized viewing of system logs. Exposes internal paths and usernames, aiding attackers in future reconnaissance.	Low

NIST

Risk Event (Vulnerability)	NIST Family	Family Code	Justification
Improper Access Control (RCE) (IBM Cloud Pak System)	Access Control	AC	The core failure is AC-3 (Access Enforcement). The application fails to restrict the attacker's access to the Class Loader, allowing unauthorized execution of code (RCE).
Path Traversal (IBM Watson Speech Services)	System and Information Integrity	SI	This is primarily an Input Validation failure (SI-10). The system fails to validate or sanitize the ../ characters in the input, allowing the user to traverse the file system.
HTTP Response Splitting (WebSphere Edge Caching Proxy)	System and Information Integrity	SI	Similar to path traversal, this is an Input Validation failure (SI-10). The application fails to sanitize CRLF (\r\n) characters, allowing the injection of malicious headers.

Weak TLS Cryptography **(IBM DataPower Gateway)**	**System and Communications Protection**	**SC**	**This falls under SC-13 (Cryptographic Protection) and SC-8 (Transmission Confidentiality). The system is using outdated algorithms to protect data in transit.**
Log Viewer Disclosure **(IBM PureApplication System)**	**Audit and Accountability**	**AU**	**While this is an access issue, NIST specifically categorizes the protection of log data under AU-9 (Protection of Audit Information). The system failed to protect audit records from unauthorized access.**

Y1- CVE: CVE-2022-24785

Asset: IBM Cloud Pak for Integration

IBM Cloud Pak for Integration is a comprehensive integration platform that connects applications, services, and data across hybrid and multi-cloud environments. Because it acts as a central integration hub, a successful attack can impact many dependent systems at once.

Vulnerability: Cross-Site Scripting (XSS)

Attack Description

The vulnerability allows attackers to inject malicious scripts into web interfaces of IBM Cloud Pak for Integration. When users or administrators access the affected interface, the script executes in their browser context.

STRIDE Analysis

Spoofing (S):

The attacker steals session cookies using XSS, allowing them to impersonate legitimate users or administrators without proper authentication.

Repudiation (R):

Actions performed using stolen sessions appear as if they were executed by legitimate users, making malicious activity difficult to trace.

Elevation of Privilege (E):

If an administrator's session is compromised, the attacker gains elevated privileges and can access or modify multiple connected integrations and services.

Likelihood: 4 / 5 (Likely)

The vulnerability can be exploited remotely, requires no special permissions, and relies on common attack techniques.

Impact: 4 / 5 (Major)

Successful exploitation enables unauthorized access, manipulation of integrations, and disruption of interconnected services.

Total Risk: 16 / 25 (High)

DREAD Analysis

Damage (9): Malicious scripts can spread across users and integrations.

Reproducibility (7): Exploitation can be repeated reliably.

Exploitability (7): XSS payloads are easy to generate and deploy.

Affected Users (9): All users accessing the affected interface may be impacted.

Discoverability (7): XSS flaws are easy to identify through testing.

Final DREAD Score: 39 / 50 (Critical)

Y2 CVE: CVE-2024-45086

Asset: IBM WebSphere Application Server

IBM WebSphere Application Server (WAS) is an enterprise Java application server used to host mission-critical business applications across cloud and hybrid environments.

Vulnerability

XML External Entity (XXE) Injection

Attack Description

The vulnerability allows attackers to exploit unsafe XML parsing, enabling unauthorized access to internal files or system resources.

STRIDE Analysis

Information Disclosure (I):

An attacker can extract sensitive information such as configuration files, credentials, or internal system data.

Denial of Service (D):

By submitting malicious XML payloads or oversized requests, the attacker can exhaust system resources and disrupt application availability.

Likelihood: 2 / 5 (Unlikely)

The attack requires specific conditions and vulnerable XML processing endpoints.

Impact: 5 / 5 (Severe)

Exploitation may result in sensitive data exposure or complete service disruption.

Total Risk: 10 / 25 (Medium)

DREAD Analysis

Damage (9): Exposure of internal files and service disruption.

Reproducibility (5): Requires correct XML endpoints and payloads.

Exploitability (7): XXE is well-known and supported by tools.

Affected Users (10): All hosted applications and users are impacted.

Discoverability (4): Requires knowledge of XML processing paths.

Final DREAD Score: 35 / 50 (Critical)

Y3-CVE: CVE-2025-0966

Asset: IBM Infosphere Information Server 11.7

IBM InfoSphere Information Server is a centralized platform for managing, transforming, and distributing trusted enterprise data.

Vulnerability

SQL Injection

Attack Description

The vulnerability allows attackers to inject malicious SQL statements into backend queries, compromising stored enterprise data.

STRIDE Analysis

Tampering (T):
Attackers can modify, insert, or delete database records. Because InfoSphere distributes data as trusted, manipulated data propagates to downstream systems.

Information Disclosure (I):
Sensitive enterprise data can be extracted directly from backend databases.

Likelihood: 3 / 5 (Moderate)

Impact: 5 / 5 (Severe)

Attackers gain full control over critical business data.

Total Risk: 15 / 25 (High)

DREAD Analysis

Damage (9): Full compromise of enterprise data integrity.

Reproducibility (9): Payloads can be reused indefinitely.

Exploitability (9): SQL injection is widely understood and automated.

Affected Users (9): All data consumers are impacted.

Discoverability (9): Vulnerable inputs are easily detected.

Final DREAD Score: 45 / 50 (Critical)

Y4-Assumption

Asset: IBM Cloud Virtual Private Cloud (VPC)

IBM Cloud VPC provides isolated private networking environments for hosting sensitive workloads.

Vulnerability

Third-Party Integration Weaknesses

STRIDE Analysis

Information Disclosure (I):

Attackers exploit vulnerabilities in integrated third-party services to access sensitive data within private cloud workloads.

Likelihood: 2 / 5 (Unlikely)

Direct attacks on VPC are difficult; exploitation depends on weaknesses in connected services.

Impact: 5 / 5 (Severe)

Sensitive data hosted within private workloads may be exposed.

Total Risk: 10 / 25 (Medium)

DREAD Analysis

Damage (9): Exposure of sensitive cloud workloads.

Reproducibility (6): Depends on third-party weaknesses.

Exploitability (6): Requires indirect attack paths.

Affected Users (5): Limited to private cloud tenants.

Discoverability (7): Third-party issues are often publicly documented.

Final DREAD Score: 33 / 50 (High)

Y5 – CVE: CVE-2025-3357

Asset: IBM Tivoli Monitoring

IBM Tivoli Monitoring is used to monitor system performance, availability, and security events across enterprise environments.

Vulnerability

Remote Code Execution due to Improper Input Validation

Vulnerability Description

IBM Tivoli Monitoring contains a vulnerability caused by improper validation of input values. A remote attacker can exploit this flaw by sending specially crafted requests, allowing the execution of arbitrary code within the monitoring service.

STRIDE Analysis

Spoofing (S):

The attacker can send malicious requests that appear legitimate to the monitoring system, effectively masquerading as trusted input sources.

Repudiation (R):

Because the malicious activity may not be clearly logged, the attacker can execute actions without reliable audit trails, making attribution difficult.

Information Disclosure (I):

Successful exploitation may allow attackers to access sensitive monitoring data, internal system information, or configuration details.

Elevation of Privilege (E):

By executing arbitrary code, the attacker gains the same privileges as the monitoring service, which can lead to full system compromise and potential lateral movement.

Likelihood: 4 / 5 (Likely)

The vulnerability is remotely exploitable, requires no user interaction, and has low attack complexity, making exploitation feasible in real environments.

Impact: 5 / 5 (Severe)

Exploitation enables remote code execution, which can compromise confidentiality, integrity, and availability of the monitoring system and connected resources.

Total Risk: 20 / 25 (Critical)

DREAD Analysis

Damage (9): Full compromise of the monitoring system and potential impact on connected infrastructure.

Reproducibility (8): The attack can be reliably repeated using the same exploit method.

Exploitability (8): Low complexity and remote accessibility make vulnerability easy to exploit.

Affected Users (8): All monitored systems and administrators may be impacted.

Discoverability (7): The vulnerability is publicly documented and discoverable.

Final DREAD Score: 40 / 50 (Critical)

Threat Propagation matrix

Component (Source)	Entry Point	Initial Threat	Propagation Mechanism (Cascade)	Final Impact Scope
IBM Cloud Pak for Integration	Web UI, APIs, Integration Endpoints	(XSS)	Malicious script steals sessions → access integrated services	Business disruption, data/session compromise across services
IBM WebSphere Application Server	Java endpoints, admin console	Attacking/exploiting java libraries	Exploit WAS → compromise hosted applications or overload services	Sensitive data leakage, DoS of enterprise apps

IBM InfoSphere Information Server 11.7	**APIs, ETL pipelines, Web inputs**	**(SQLi/XSS)**	**Database compromise → corrupted data propagates to consumers**	**Enterprise-wide data integrity & confidentiality loss**
IBM Cloud VPC	**Third-party APIs & integrations**		**Exploit third-party service → pivot into VPC workloads**	**Exposure of sensitive workloads and private data**
IBM Tivoli Monitoring	**Admin & monitoring consoles**		**Admin compromise → execute commands across monitored systems**	**Full environment compromise, credential theft**

Contextual Risk Register

Risk Event	Context (Asset / Process)	Business Impact	Real Score
Cross-Site Scripting (XSS)	**IBM Cloud Pak for Integration**Acts as a central integration hub connecting applications, services, and data across hybrid and multi-cloud environments. A compromise can cascade across dependent systems.	Attackers inject malicious scripts into management interfaces, enabling session hijacking of users or administrators. This can result in unauthorized access, manipulation of integrations, and disruption of multiple connected services.	**High**
XML External Entity (XXE) Injection	**IBM WebSphere Application Server**Enterprise Java application server hosting mission-critical business applications across cloud and hybrid infrastructures.	Exploitation exposes internal configuration files, credentials, or system resources. Malicious XML payloads can also exhaust resources, causing service outages affecting all hosted applications.	**High**
SQL Injection	**IBM InfoSphere Information Server 11.7**Centralized platform for managing, transforming, and distributing trusted enterprise data across downstream systems.	Attackers gain unauthorized access to backend databases, allowing modification or extraction of critical enterprise data. Manipulated data propagates to dependent systems, impacting data integrity enterprise wide.	**Very High**
Third-Party Integration Weaknesses	**IBM Cloud Virtual Private Cloud (VPC)**Provides isolated private networking environments for hosting sensitive workloads in the cloud.	Vulnerabilities in integrated third-party services allow indirect access to sensitive private workloads, leading to data exposure despite VPC isolation controls.	**High**
Remote Code Execution (Improper Input Validation)	**IBM Tivoli Monitoring**Monitors system performance, availability, and security events across enterprise infrastructure.	Remote attackers to execute arbitrary code within the monitoring service, gaining privileged access. This enables compromise of monitoring data, manipulation of alerts, and lateral movement into monitored systems.	**Very High**

Nist

Risk Event (Vulnerability)	NIST Family	Family Code	Justification
Cross-Site Scripting (XSS)(IBM Cloud Pak for Integration)	**Access Control**	**AC**	**The core failure relates to AC-3 (Access Enforcement). XSS enables session hijacking, allowing attackers to bypass authentication and impersonate legitimate users or administrators, gaining unauthorized access to integration services.**
Cross-Site Scripting (XSS)(IBM Cloud Pak for Integration)	**System and Information Integrity**	**SI**	**This vulnerability is also a violation of SI-10 (Information Input Validation). The system fails to properly sanitize and encode user input, allowing malicious scripts to be injected and executed in users' browsers.**
XML External Entity (XXE) Injection(IBM WebSphere Application Server)	**System and Information Integrity**	**SI**	**The vulnerability represents a failure of SI-10 (Input Validation) and SI-7 (Integrity Mechanisms). Unsafe XML parsing allows attackers to read internal files or trigger denial-of-service conditions.**
SQL Injection(IBM InfoSphere Information Server)	**System and Information Integrity**	**SI**	**SQL injection directly violates SI-10 (Information Input Validation). The application does not validate or parameterize database queries, allowing attackers to manipulate backend databases and enterprise data flows.**
SQL Injection(IBM InfoSphere Information Server)	**Access Control**	**AC**	**The attack also demonstrates weak AC-6 (Least Privilege). Excessive database permissions allow injected queries to modify, delete, or extract sensitive enterprise data beyond intended access levels.**
Third-Party Integration Weaknesses(IBM Cloud Virtual Private Cloud)	**Supply Chain Risk Management**	**SR**	**This risk maps to SR-3 (Supply Chain Controls and Processes). Weak security in third-party services introduces indirect attack paths into otherwise isolated VPC environments.**
Third-Party Integration Weaknesses(IBM Cloud Virtual Private Cloud)	**System and Communications Protection**	**SC**	**The vulnerability also reflects weaknesses in SC-7 (Boundary Protection), where trusted integrations are not sufficiently isolated, enabling data exposure through connected services.**
Remote Code Execution (Improper Input Validation)(IBM Tivoli Monitoring)	**System and Information Integrity**	**SI**	**The primary failure is SI-10 (Input Validation). Improper validation of input values allows attackers to inject malicious payloads that result in arbitrary code execution.**
Remote Code Execution (Improper Input Validation)(IBM Tivoli Monitoring)	**Access Control**	**AC**	**The exploit violates AC-6 (Least Privilege). The monitoring service executes injected code with excessive privileges, enabling full system compromise and lateral movement.**
Remote Code Execution (Improper Input Validation)(IBM Tivoli Monitoring)	**Audit and Accountability**	**AU**	**Weak or insufficient logging violates AU-2 (Event Logging). Malicious actions may not be adequately recorded, allowing attackers to execute code without reliable attribution.**

K1-Security Bulletin: Server-Side Request Forgery via Axios URL Parsing Flaw (CVE-2024-39338)

Asset: IBM Cloud Pak for integration

Vulnerability: Server-Side Request Forgery (SSRF) allowing bypass of network access controls

Initial Access: The attacker identifies a user-controlled field processed by axios (e.g., webhook URL configuration) and injects a malicious payload starting with

Exploitation: Axios incorrectly processes path-relative URLs as protocol-relative URLs. Because input validation is missing, the system routes the request to internal hosts, bypassing firewall rules and network segmentation.

Spoofing: Attackers can spoof internal service requests.

Information Disclosure: Exfiltrates data from internal services

Post-Exploitation: Exposed credentials allow the attacker to escalate privileges, pivot to move laterally within the cloud infrastructure, and compromise internal components.

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Repudiation: Attackers can spoof internal service requests. Information Disclosure: Exfiltrates data from internal services.

Likelihood: 4/5 Axios is a widely used dependency; many services process user-supplied URLs, and the attack requires minimal skill.

Impact: 4/5 SSRF can lead to complete cloud environment compromise through metadata service access, violating fundamental security boundaries.

Total Risk = 4 * 4 = 16 → High Risk

DREAD Analysis

Damage: 9/10 Attackers can reach internal metadata services, steal cloud credentials, and pull data from internal databases.

Reproducibility: 8/10 The axios bug triggers crafted URLs every time and affects all deployments using the vulnerable version.

Exploitability: 8/10 Attackers only need basic HTTP crafting, and standard SSRF tools work without authentication.

Affected Users: 7/10 All Cloud Pak for Data tenants are exposed, putting co-located customers and enterprise analytics teams at risk.

Discoverability: 9/10 URL parameters are common targets, and the flaw appears during routine fuzzing on both authenticated and unauthenticated endpoints.

Total: 41 / 50 → Critical Risk

K2-Security Bulletin: Container Escape via container Race Condition (CVE-2024-45310)

Asset: IBM Cloud Kubernetes Service Worker Nodes (Web Server)

Vulnerability: Container Escape and Privilege Escalation via TOCTOU race condition

Initial Access: The attacker deploys a pod with a specially crafted volume mount configuration.

Exploitation: A Time-of-Check Time-of-Use (TOCTOU) race condition exists in the run volume of mount logic. The attacker exploits the timing gap between validation and mount operations by creating symbolic links that resolve host paths.

Tampering: Creates unauthorized files on host.

Elevation of Privilege: Escapes container isolation.

Post-Exploitation: The attacker gains unauthorized access to the host filesystem, creating arbitrary files or directories, which allows for privilege escalation and lateral movement to other containers.

CVSS Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

Repudiation: Creates unauthorized files on the host system. Information Disclosure: Escapes container isolation to access host-level data.

Likelihood: 2/5 Requires specific timing conditions and local access; race conditions are difficult to reliably exploit and depend on system load.

Impact: 3/5 Container escape violates fundamental security boundaries and could lead to cluster-wide compromise if combined with other vulnerabilities.

Total Risk = 2 * 3 = 6 → Medium Risk

DREAD Analysis

Damage: 8/10 Breaking container isolation grants access to the full worker node, allowing attackers to reach secrets from other containers and weaken the multi-tenant security model.

Reproducibility: 4/10 The race condition depends heavily on timing, system load, and scheduling, often requiring multiple attempts to succeed.

Exploitability: 3/10 Attackers require knowledge of runtime internals, access to deploy pods, specific volume setups, and precise timing.

Affected Users: 6/10 A compromised node affects all pods hosted on it, and the shared node design allows attackers to move across namespaces.

Discoverability: 5/10 Attackers need Kubernetes API access; the flaw is not reachable by external scans and typically requires code review or debugging to find.

Total: 26 / 50 → Medium-High Risk

K3-Security Bulletin: Mountable Secrets Policy Enforcement Bypass (CVE-2024-3177)

Asset: IBM Cloud Kubernetes Service Clusters (IBM Cloud services)

Vulnerability: Security Policy Bypass failing to enforce mountable secret policies

Initial Access: The attacker authenticates to the Kubernetes cluster with a limited-service account and creates a pod specification referencing restricted secrets in the envFrom field.

Exploitation: The kube-apiserver (specifically the Service Account admission plugin) fails to validate secret mounts via the envFrom field. This allows the pod to be created without applying the mountable secrets policy.

Information Disclosure: Unauthorized access to database credentials, API keys, TLS certificates, and authentication tokens for service accounts.

Post-Exploitation: Attackers can use extracted credentials for lateral movement within the cluster, compromise dependent services, and access sensitive configuration data.

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N

Repudiation: Audit trail gaps occur due to the policy bypass. Information Disclosure: Unauthorized secret access occurs.

Likelihood: 2/5 Requires authenticated access and specific pod creation privileges; the scope is limited to the namespace, and a patch is readily available.

Impact: 2/5 Impact is limited to secrets within the same namespace; it does not provide cluster-admin access and can be mitigated by RBAC policies.

Total Risk = 2 * 2 = 4 → Low Risk

DREAD Analysis

Damage: 5/10 Attackers only reach secrets in the same namespace; there is no cluster-wide credential theft or host access, keeping impact within one tenant.

Reproducibility: 9/10 A crafted pod spec triggers the bypass consistently across affected kube-apiserver versions.

Exploitability: 4/10 Attackers require authenticated Kubernetes access and RBAC rights to create pods and understand secret mounting.

Affected Users: 4/10 Only workloads in the same namespace are exposed; there is no effect across tenants in a properly isolated cluster.

Discoverability: 6/10 Audits and policy tests highlight the issue; the pattern is known and easy to verify with valid credentials.

Total: 28 / 50 → Medium Risk

K4-Security Bulletin: CRI-O Container Restore Validation Bypass (CVE-2024-8676)

Asset: Red Hat OpenShift Cluster Worker Nodes on IBM Cloud (VPC Boundaries)

Vulnerability: Privilege Escalation and Access Control Bypass via improper restore validation

Initial Access: The attacker gains access to a node with kubelet or cri-o socket privileges.

Exploitation: CRI-O fails to validate container specifications during restore operations. It uses mount information from checkpoint archives without re-validating against host mount access controls, allowing the attacker to bypass security policies using a crafted archive.

Tampering: Modifies container mount specifications.

Information Disclosure: Sensitive host configuration and host filesystem data.

Elevation of Privilege: Escalate from container to host.

Post-Exploitation: A successful exploit leads to complete container escape, allowing the attacker to access the host filesystem, modify host settings, and potentially breach the entire cluster.

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Repudiation: Modifies container mount specifications. Information Disclosure: Access to host filesystem data.

Likelihood: 1/5 Requires direct node access and socket privileges; attack complexity is high, and exposure is limited in managed IBM Cloud environments.

Impact: 5/5 Complete container escape leads to host compromise, affects the entire cluster, and violates fundamental isolation guarantees.

Total Risk = 1 * 5 = 5 → High Risk

DREAD Analysis

Damage: 10/10 A successful exploit allows full escape from the container, giving unrestricted host filesystem access and control-plane escalation potential.

Reproducibility: 3/10 The attack depends on a specific checkpoint and restores flow, state and timing constraints, and requires specific node privileges.

Exploitability: 2/10 Attackers need deep CRI-O and OpenShift knowledge to craft malicious checkpoint archives; only highly privileged users can attempt this.

Affected Users: 7/10 A breached node endangers every workload on it; node credentials may allow escalation to cluster-admin, exposing the multi-tenant environment.

Discoverability: 3/10 Attackers need internal access; external scans cannot find this pathway, and the flaw typically appears only through code review.

Total: 25 / 50 → Medium Risk

K5-Security Bulletin: BCryptPasswordEncoder Length Truncation Authentication Bypass (CVE-2025-22228)

Asset: Web Server & WebSphere

Vulnerability: Authentication Bypass via cryptographic validation flaw

Initial Access: The attacker, having obtained a password hash, crafts a password longer than 72 characters and submits it to the authentication endpoint.

Exploitation: The BCryptPasswordEncoder implementation incorrectly validates passwords by checking only the first 72 bytes. The system accepts over-length passwords that collide with the first 72 bytes of the legitimate password, allowing a bypass of authentication controls.

Spoofing: Impersonates legitimate user identity.

Information Disclosure: Stored objects, files, and metadata belonging to customers.

Elevation of Privilege: Gains administrative access

Post-Exploitation: The attacker gains unauthorized administrative access, allowing them to manipulate storage buckets, modify or delete data, change storage policies, and execute a large-scale data breach.

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Repudiation: Impersonates legitimate user identity. Information Disclosure: Access to stored objects and metadata.

Likelihood: 2/5 Requires hash disclosure and collision crafting; attack complexity is high, limiting it to systems using specific BCryptPasswordEncoder configurations.

Impact: 5/5 Complete administrative compromise of object storage leads to potential massive data breaches affecting multiple customers in a multi-tenant environment.

Total Risk = 2 * 5 = 10 → High Risk

DREAD Analysis

Damage: 9/10 A successful bypass grants full control of IBM Cloud Object Storage, enabling attackers to read and change all buckets and policies, leading to a large-scale data breach.

Reproducibility: 7/10 The truncation flaw works consistently once the target hash is known and affects all accounts using the vulnerable component.

Exploitability: 5/10 Attackers must first obtain the password hash through another flaw or leak, analyze it, and craft a colliding over-length password.

Affected Users: 9/10 Object Storage supports many enterprise customers; a single bypass could expose multiple accounts sharing the same backend, leading to severe regulatory consequences.

Discoverability: 6/10 The issue appears during authenticated testing or cryptographic analysis rather than external scans; only users with account access or deep inspection capabilities can uncover it.

Total: 36 / 50 → High-Critical Risk

Threat Propagation Matrix:

Component (Source)	**Entry Point**	**Vulnerability Type**	**Propagation Mechanism (The Cascade)**	**Target / Final Impact Scope**
Axios HTTP Client (IBM Cloud Pak for integration)	**Webhook Config / URL Input**	**Server-Side Request Forgery (SSRF)**	SSRF pivots request from App Layer $\rightarrow$ Network Layer $\rightarrow$ Metadata Service.	**Cloud Infrastructure:** Compromise of IAM Credentials and lateral movement within the VPC.
containerd / runc (Web Server)	**Malicious Pod Volume Mount**	**Race Condition (TOCTOU)**	Filesystem escape moves from Container Context $\rightarrow$ Host Kernel Space via symbolic link timing attack.	**Shared Worker Node:** Compromise of the physical/virtual node and all co-located tenant pods.
kube-apiserver (IBM Cloud services)	**Pod Manifest (envFrom field)**	**Policy Bypass (Admission Control)**	Bypass flows from Admission Control $\rightarrow$ Pod Runtime $\rightarrow$ External Services by ignoring secret mount policies.	**Dependent Services:** Unintended access to external databases or APIs via leaked credentials.
CRI-O Runtime (VPC Boundaries)	**Crafted Checkpoint Archive**	**Restore Validation Bypass**	Restore Logic Bypass flows from Checkpoint Data $\rightarrow$ Runtime Configuration $\rightarrow$ Host Filesystem.	**Cluster Integrity:** Full breach of node integrity and violation of multi-tenant isolation.

Spring Security Web Server & WebSphere)	**Login Password Input Field**	**Authentication Bypass (Truncation)**	Auth Bypass flows from Identity Provider $\rightarrow$ Management Console $\rightarrow$ Data Plane via hash collision.	**Data Estate:** Massive data breach or data loss across multiple storage buckets/tenants.

Contextual Risk Register:

Risk Event (Vulnerability)	Asset Context & Description	Criticality Rationale (Why is this Asset Critical?)	Business Impact	Real Score
SSRF / Metadata Access (CVE-2024-39338)	**Asset:** IBM Cloud Pak for integration **Description:** A central platform for processing sensitive customer PII and connecting to internal data services.	**CRITICAL:** This asset acts as the organization's "Data Brain." Compromising it isn't just a service outage; it is a direct path to the **Metadata Service** and IAM credentials, exposing the most protected data classes.	Attackers bypass network controls, leading to massive data exfiltration. This directly triggers **GDPR fines** (up to 4% of revenue) and catastrophic loss of customer trust.	**CRITICAL**
Admin Auth Bypass (CVE-2025-22228)	**Asset:** Web Server & WebSphere **Description:** The object storage system housing immutable financial logs, backups, and "Gold Copy" records.	**CRITICAL:** This asset is the "Vault." The business relies entirely on this for Disaster Recovery (DR). Unauthorized administrative access here essentially hands over the keys to the entire kingdom.	Authentication bypass allows attackers to delete or encrypt (Ransomware) immutable records. Loss of this data is an **existential business threat** preventing financial reconciliation.	**CRITICAL**
Container Escape (CVE-2024-45310)	**Asset:** IBM Cloud Kubernetes Service Worker Nodes (Web Server) **Description:** A shared worker node hosting payment processing	**HIGH:** The environment is **Shared/Multi-tenant**. Isolation is the only security layer here. If isolation breaks, the attacker moves from one tenant to the	A race condition allows writing to the host filesystem[7]. This violates **PCI DSS segmentation** requirements, compromising the integrity of all payment transactions on that node.	**HIGH**

	containers for multiple tenants.	Host OS, and then to all other tenants.		
Runtime Tampering (CVE-2024-8676)	**Asset:** Red Hat OpenShift Cluster Worker Nodes on IBM Cloud (VPC Boundaries) **Description:** A cluster dedicated to processing operational logs and audit trails using the CRI-O runtime.	**HIGH:** This asset safeguards **Integrity**. If analytics and audit logs can be tampered with, security teams become blind to other attacks.	Malicious checkpoint restoration grants host access. Tampering with audit logs violates **SOX compliance** regarding financial reporting integrity.	**HIGH**
Secret Policy Bypass (CVE-2024-3177)	**Asset:** IBM Cloud Kubernetes Service Clusters (IBM Cloud services) **Description:** An isolated namespace used by developers for testing code. It contains no production data.	**MEDIUM:** The asset is **Logically Isolated**. While the vulnerability is technically real, it affects a sandbox environment. There is no PII or financial data to steal.	Attackers access secrets outside their intended scope. However, since this is a Test environment, financial loss is negligible, and impact is contained to the sandbox.	**MEDIUM**

NIST 800-53 Control Family Mapping:

CVE ID	Vulnerability Name	NIST Family	Specific Control (Ref)	Justification
CVE-2024-39338	**Cloud Pak SSRF**	**SI (System and Information Integrity)**	**SI-10: Information Input Validation**	**The root cause is Axios failing to validate protocol-relative URLs (//...) before processing them. Proper input validation would prevent the SSRF payload from executing.**
CVE-2025-22228	**Object Storage Auth Bypass**	**IA (Identification and Authentication)**	**IA-5: Authenticator Management**	**The flaw lies in the BCryptPasswordEncoder truncating passwords, allowing authentication bypass. This is a direct failure of the system's ability to verify user identity securely.**

CVE-2024-45310	**Container Runtime Escape**	**SC (System and Communications Protection)**	**SC-39: Process Isolation**	**The vulnerability allows a process to "escape" the container sandbox and write to the host filesystem. This violates the requirement to maintain logical isolation between tenant workloads.**
CVE-2024-3177	**K8s Policy Bypass**	**AC (Access Control)**	**AC-3: Access Enforcement**	**The Kubernetes API server fails to enforce policies regarding "mountable secrets". The system failed to check if the requesting Pod was authorized to access specific secrets.**
CVE-2024-8676	**OpenShift Restore Attack**	**AC (Access Control)**	**AC-6: Least Privilege**	**The cri-o runtime grants excess privileges (host mounts) during the restore process by trusting the checkpoint data without re-validation. This bypasses the intended privilege restrictions.**

J1 - CVE-2024-38747: Sensitive Data Exposure in Payment Gateway Logs

Asset: Cloud Logging and Monitoring Database (Payment Platform)

Vulnerability: Sensitive Data Exposure in Log Files

Initial Access:

The attacker sends a direct HTTP request to the log viewer URL or accesses publicly exposed log files through misconfigured cloud storage buckets.

Exploitation:

Because access controls are missing or improperly configured, the system returns log files to an unauthorized user without authentication. Depending on configuration, logs may include payment identifiers, customer details, API responses, error traces, or partial credential-like data that can aid further attacks.

Information Disclosure:

The primary threat is unauthorized access to sensitive log data—payment metadata, user identifiers, internal API URLs, and possible secrets—which should be restricted to a small set of admin or security roles.

Post-Exploitation:

With access to payment logs, the attacker can identify payment patterns, extract customer information, discover API endpoints, and potentially extract session tokens or temporary credentials that were inadvertently logged.

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

STRIDE Analysis:

Spoofing (S): If logs contain exposed tokens, API keys, or session identifiers, an attacker can replay them to impersonate legitimate services or users against payment APIs.

Information Disclosure (I): The primary threat is unauthorized access to sensitive log data—payment metadata, user identifiers, internal API URLs, and possible secrets—which should be restricted to a small set of admin or security roles.

Tampering (T): While the core vulnerability is read-only, knowledge gained from logs (internal paths, parameters, and error behaviors) can be used to craft precise SQL injection, deserialization, or authentication-bypass attacks that tamper with payment records in the primary database.

Repudiation (R): If log access is broad and poorly audited, attackers who later manipulate payment data can plausibly deny involvement, and defenders may struggle to reconstruct accurate timelines because logs were exposed and potentially selectively deleted or overridden by someone with illegitimate access.

Likelihood: 3 / 5

Misconfigured log ACLs are common in cloud environments, especially when logs are stored in shared buckets or logging clusters. However, exploitation usually requires at least some level of access to the environment (for example, a compromised low-privilege account or insider), not purely anonymous internet access**.**

Impact: 4 / 5

Exposed logs can reveal payment flows, customer data, error codes, and internal design details valuable for fraud or deeper technical compromise. If logs contain any secrets (tokens, API keys, password-like values), the exposure can escalate into direct compromise of payment APIs or databases.

Total Risk: 12 / 25 (Medium–High)

DREAD Analysis:

Damage (7/10): Leaked logs can enable targeted fraud, account takeover, and technical exploitation of backend APIs; actual damage depends on whether true secrets or card data are logged.

Reproducibility (7/10): Once an attacker knows where logs are stored and has sufficient access, reading them is trivial and repeatable; misconfigured ACLs persist until fixed.

Exploitability (5/10): Requires some foothold (misconfigured permissions, compromised low-privilege account, or open log bucket), but no advanced exploit code; basic HTTP or storage access tools are enough.

Affected Users (7/10): Potentially all customers whose transactions or accounts pass through the payment system during the affected period, since central logging typically touches every request.

Discoverability (4/10): Misconfigured ACLs on internal logging backends are less obvious from the outside and typically require either inside knowledge or broad environment scanning to detect.

Final DREAD Score: 30 / 50 (Medium–High)

J2 - CVE-2019-4225: Sensitive Data in Log Files

Asset: IBM PureApplication System (2.2.3.0–2.2.5.3)

Vulnerability: Sensitive Data in Log Files

Initial Access:
Attacker gains low-privilege local access (for example, support account, compromised application user, or maintenance script).

Exploitation:
Attacker reads application and system logs under directories accessible to local users. Attacker harvests database connection strings, passwords, API keys, or internal hostnames from log entries.

Post-Exploitation:
Attacker uses this information to pivot to databases, management of UIs, or external services. With harvested

credentials and internal topology information, the attacker can launch targeted attacks against dependent systems that would normally be protected by network boundaries.

Information Disclosure:
The core issue is unauthorized access to sensitive information (credentials, configuration, internal topology) stored in log files that are readable beyond the intended audience.

CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

STRIDE Analysis:

Information Disclosure (I): The core issue is unauthorized access to sensitive information (credentials, configuration, internal topology) stored in log files that are readable beyond the intended audience.

Spoofing (S): If credentials or tokens are logged, the attacker can reuse them to impersonate service accounts or administrators on dependent systems (for example, databases, LDAP, or cloud APIs).

Tampering (T): With harvested credentials, the attacker can connect to downstream systems and modify data or configurations (for example, change application parameters, alter patterns, or update database records), even though the PureApplication vulnerability itself is read-only.

Elevation of Privilege (E): A low-privilege local user can escalate their effective privileges in the wider environment by using leaked admin or service-account credentials to access higher-privilege components outside their original role.

Likelihood: 3 / 5

Requires local access to the PureApplication System (console, SSH, or application user shell), which limits remote drive-by exploitation. However, appliances often have multiple operators, support users, and application-level accounts that may be able to reach log directories.

Impact: 3 / 5

Direct impact is indirect compromise via leaked information: the vulnerability itself does not change data or execute code, but exposes secrets, internal paths, and operational details. If credentials in logs are reused for critical systems (databases, LDAP, cloud APIs), the impact can escalate to major.

Total Risk: 9 / 25 (Medium)

DREAD Analysis:

Damage (4/10): Leaked credentials and configuration can enable further compromise of databases and management interfaces but do not by themselves destroy or alter data on the appliance.

Reproducibility (7/10): Once local access is obtained, log reading is straightforward and repeatable; any user with similar access can repeat the attack as long as logs contain sensitive data.

Exploitability (5/10): The technical barrier is low (viewing log files), but the need for local access raises the bar compared to a pure remote exploit.

Affected Users (6/10): All applications and tenants whose credentials or details are logged on the affected system can be impacted, but scope is limited to what is written into the logs.

Discoverability (6/10): Security testing tools and manual reviewers can detect sensitive data in logs fairly easily; the vulnerability is documented and has a public CVE entry and IBM security bulletin.

Final DREAD Score: 28 / 50 (Medium)

J3 - CVE-2025-61757: Oracle Identity Manager Pre-Auth RCE

Asset: Oracle Identity Manager (OIM) – IAM Infrastructure

Vulnerability: Pre-Authentication Remote Code Execution

Initial Access:
The attacker identifies an unpatched Oracle Identity Manager instance and crafts a malicious WADL (Web Application Description Language) payload that exploits the authentication bypass.

Exploitation:
By appending metadata-style suffixes such as ;.wadl or ?WSDL to REST URIs, an attacker can bypass the authentication filter and reach protected API handlers. After bypassing the filter, the attacker reaches an exposed Groovy script endpoint meant for checking Groovy code. By writing an annotation that executes at compile time, the attacker achieves arbitrary code execution.

Remote Code Execution:
Full RCE on the OIM server enables the attacker to execute arbitrary system commands and Java code within the WebLogic application server context.

Post-Exploitation:
Full compromise of the OIM server enables the attacker to modify or create privileged accounts, tamper with provisioning workflows, interfere with MFA/SSO or downstream identity systems, establish persistence on the WebLogic/OIM host, and move laterally into connected directories and SaaS identity integrations. All 2.4 million users' access can be modified; tokens can be revoked, and complete administrative control is achieved.

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

STRIDE Analysis:

Spoofing (S): The attacker bypasses authentication entirely, allowing them to impersonate any user or administrator without proper credentials.

Tampering (T): With RCE access, the attacker can modify IAM policies, create backdoor accounts, alter provisioning workflows, and change MFA settings.

Repudiation (R): Actions performed via RCE can be disguised as legitimate system operations, making forensic analysis difficult.

Information Disclosure (I): Complete access to IAM database containing all user credentials, service accounts, API keys, and OAuth tokens for connected systems.

Denial of Service (D): The attacker can crash the IAM service, disrupting authentication for all enterprise applications.

Elevation of Privilege (E): Unauthenticated attacker escalates to full administrative control of the identity platform, enabling creation of domain admin accounts and compromise of all connected systems.

Likelihood: 4 / 5

CISA has added this to the Known Exploited Vulnerabilities (KEV) catalog, confirming active exploitation in the wild. The vulnerability requires no authentication, low attack complexity, and public proof-of-concept exploits are available.

Impact: 5 / 5

Complete IAM takeover without authentication enables all STRIDE categories, affecting all 2.4 million users and all connected enterprise systems. Business impact includes platform shutdown, regulatory violations (PCI DSS, GDPR, SOX), and potential bankruptcy-level financial damage.

Total Risk: 20 / 25 (CRITICAL)

DREAD Analysis:

Damage (10/10): Complete IAM platform compromise enables creation of privileged accounts, modification of all policies, and access to all connected systems across the enterprise.

Reproducibility (10/10): Works every time with a simple HTTP request; public PoC available and confirmed exploitation in the wild.

Exploitability (10/10): No authentication required, network accessible, trivial HTTP manipulation using standard tools.

Affected Users (10/10): All 2.4 million users of the IAM platform and all connected enterprise systems are affected.

Discoverability (8/10): Authentication bypass techniques are well-documented; public vulnerability databases list the affected versions and attack methods.

Final DREAD Score: 48 / 50 (Critical)

J4 - CVE-2025-1094: PostgreSQL psql SQL Injection

Asset: PostgreSQL Database (psql Interface) - IAM infrastructure

Vulnerability: SQL Injection via Interactive Terminal Input

Initial Access:
The attacker connects to a PostgreSQL database using psql with credentials obtained through social engineering, credential stuffing, or misconfigured default credentials.

Exploitation:
The attacker exploits insufficient input sanitization in the psql interactive terminal. By injecting SQL commands through specially crafted input strings, the attacker bypasses intended query boundaries and executes unintended SQL operations.

SQL Injection Attack:
The attacker constructs payloads such as ' OR '1'='1 or '; DROP TABLE users; -- to manipulate query logic or execute arbitrary SQL commands that modify data, extract sensitive information, or delete database objects.

Data Exfiltration & Manipulation:
With successful SQL injection, the attacker can execute any SQL command with the privileges of the connected user account. This allows extraction of entire databases, modification of access control lists, deletion of audit logs, or creation of unauthorized accounts.

Post-Exploitation:
The attacker establishes persistence by creating backup user accounts, modifying logging configurations to hide tracks, or installing database triggers that execute malicious code on future queries.

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

STRIDE Analysis:

Tampering (T): The attacker can modify database records, drop tables, alter stored procedures, and change access control policies through injected SQL commands.

Information Disclosure (I): The attacker can query any table accessible to the database user, extracting passwords, encryption keys, personal data, and confidential business information.

Denial of Service (D): The attacker can execute resource-intensive queries, drop critical tables, or corrupt the database, rendering it unavailable.

Repudiation (R): If database logging is insufficient, the attacker can delete audit logs to cover tracks and evade accountability.

Elevation of Privilege (E): If the compromised account has SUPERUSER or CREATEDB privileges, the attacker gains administrative control of the entire database system.

Likelihood: 4 / 5

SQL injection remains one of the most commonly exploited vulnerabilities because input validation is frequently incomplete. The attack requires only low-privilege database access and network connectivity. No complex exploit tools are required.

Impact: 4 / 5

SQL injection can lead to complete database compromise, data theft, data destruction, and service disruption. The actual impact depends on the privileges of the compromised user account and the sensitivity of data stored in the database.

Total Risk: 16 / 25 (High)

DREAD Analysis:

Damage (8/10): Can lead to complete database compromise, data theft, data destruction, and denial of service depending on attacker actions.

Reproducibility (9/10): SQL injection attacks are highly reproducible; once a vulnerable input point is identified, the attack can be repeated consistently.

Exploitability (7/10): Requires knowledge of SQL syntax and basic database structure, but no advanced technical skills; widely documented techniques and tools available.

Affected Users (8/10): All data in the database is potentially affected; all users whose information is stored in the compromised database are impacted.

Discoverability (8/10): Automated scanning tools and manual testing easily identify SQL injection vulnerabilities; the attack pattern is well-known.

Final DREAD Score: 40 / 50 (High)

J5 - CVE-2024-55949: MinIO IAM Privilege Escalation

Asset: MinIO Object Storage – IAM Database

Vulnerability: IAM Privilege Escalation via Policy Manipulation

Initial Access:
The attacker obtains initial access with a low-privileged service account or user account in the MinIO cluster. This could be through credential theft, compromised containers, or misconfigured default credentials.

Exploitation:
The attacker exploits insufficient authorization checks in MinIO's IAM policy enforcement mechanism. By crafting malicious policy documents or exploiting policy evaluation logic flaws, the attacker escalates their privileges from read-only to administrative access.

Privilege Escalation Vector:
The vulnerability may exist in:

- Policy attachment mechanisms that allow attaching admin policies to low-privilege users
- Policy evaluation logic that incorrectly interprets wildcard characters or resource identifiers
- Race conditions in concurrent policy updates that allow policy injection
- Insufficient validation of policy JSON structure that enables bypass of authorization checks

Remote Code Execution & Data Exfiltration:
With elevated privileges, the attacker can:

- Create new administrative access keys
- Read all bucket contents (potentially millions of objects)
- Delete or modify bucket policies
- Access encryption keys stored in MinIO
- Create or modify bucket configurations
- Establish persistence through backdoor service accounts

CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

STRIDE Analysis:

Elevation of Privilege (E): The core vulnerability is a privilege escalation that converts a low-privilege account into an administrative account with full cluster access.

Tampering (T): With administrative privileges, the attacker can tamper with bucket contents, policies, configurations, and store objects without authorization.

Information Disclosure (I): The attacker gains access to all objects stored in MinIO buckets, including potentially sensitive data, encryption keys, and confidential business files.

Repudiation (R): Attacker actions performed with escalated privileges can be attributed to the compromised low-privilege account, making accountability difficult if logging is insufficient.

Denial of Service (D): The attacker can delete critical buckets, objects, or configurations, causing service disruption for all dependent applications.

Likelihood: 3 / 5

The vulnerability requires initial low-privilege account access, which is a realistic scenario in multi-tenant environments. However, the privilege of escalation itself may require specific knowledge of MinIO's policy evaluation mechanisms.

Impact: 5 / 5

Administrative access to MinIO grants complete control over all stored data, configurations, and access controls. In environments using MinIO as central storage for application data, databases, or backups, the impact is catastrophic.

Total Risk: 15 / 25 (High)

DREAD Analysis:

Damage (9/10): Privilege escalation to admin grants full control over all stored data, allowing theft, deletion, or corruption of critical business data.

Reproducibility (7/10): Once the privilege of escalation method is understood, it can be repeated consistently; however, it may require specific environmental conditions.

Exploitability (6/10): Requires initial low-privilege access and knowledge of MinIO's policy mechanism; not trivial but within capability of determined attacker.

Affected Users (9/10): All data stored in the MinIO cluster is affected; all applications and users relying on that data are impacted.

Discoverability (6/10): The vulnerability requires understanding of MinIO's policy evaluation logic; automated scanners may not detect this type of authorization bypass.

Final DREAD Score: 37 / 50 (High)

Threat Propagation Matrix:

Vulnerability / Asset	Entry Point	Primary Impact	Propagation Path	Final Impact
Payment Gateway Logs	Direct URL or misconfigured log storage (no / weak auth)	Log data disclosure	Leaked logs reveal endpoints, stack traces, customer/payment metadata, and possible tokens → attacker maps internal APIs and reuses exposed secrets against payment services	Targeted fraud against payment flows, impersonation of users/services, easier exploitation of other weaknesses in the payment platform
IBM PureApplication System	Local shell / console user with access to log directories	Sensitive config and credential disclosure	Attacker reads logs → extracts DB credentials, API keys, hostnames → uses them to log into databases and admin consoles → modifies configs and data	Unauthorized access to backend systems, policy and data tampering, lateral movement across environments using leaked credentials
Oracle Identity Manager (IAM)	Public REST WebServices endpoint (pre-auth)	Full IAM RCE and takeover	Metadata-suffixed REST calls bypass auth → reach Groovy endpoint → RCE on OIM/WebLogic → attacker creates backdoor admin accounts, alters IAM policies, and controls SSO/MFA for all users	Enterprise-wide identity compromise: attackers provision privileged accounts, access all connected apps, potentially causing organization-wide breach
PostgreSQL psql (IAM)	psql interface using low-privileged DB credentials	SQL injection and data compromise	Crafted input in psql session injects arbitrary SQL → attacker dumps or alters tables, creates new DB users, deletes or corrupts logs → may escalate to SUPERUSER if role is misconfigured	Complete database compromise (C/I/A), long-term persistence via hidden accounts, and disruption of all

				services depending on this DB
MinIO (IAM)	MinIO IAM policy APIs from a low-privileged account	Privilege escalation in object storage	Flawed policy enforcement lets attacker attach or craft admin-level policies → gain full MinIO admin → read, modify, or delete any bucket/object, create rogue access keys	Loss or theft of all stored data, outage of dependent apps, and durable backdoor access through attacker-controlled IAM identities

Contextual Risk Register:

Risk Event	Context (Asset / Process)	Business Impact	Real Score
Payment Gateway Log Exposure	**Cloud Logging & Monitoring for Payment Platform**. Central store for payment transaction logs, API traces, and error diagnostics used by ops and security teams.	Exposure of payment metadata, customer identifiers, API endpoints, and possibly tokens or keys. Enables targeted fraud, replay of API calls, and preparation of deeper technical attacks against payment services.	**High**
PureApplication Log Disclosure	**IBM PureApplication System Logs**. Hosts enterprise app workloads; logs contain configuration, connection strings, and operational events for many business services.	Local users can harvest credentials and topology data, then pivot into databases and management consoles. Leads to unauthorized changes to enterprise apps and data, and stealthy lateral movement across environments.	**Medium**
Oracle Identity Manager Pre-Auth RCE	**Enterprise IAM Platform (OIM)**. Central authority for user lifecycle, roles, and access to directories, SaaS apps, and critical business systems.	Unauthenticated attacker gains full IAM admin and OS control. Can create privileged accounts, disable MFA, revoke or mint tokens, and compromise every integrated application, causing organization-wide breach and outages.	**Very High**
PostgreSQL SQL Injection	**Core Relational Database** backing business applications and reports. Accessed via psql by admins and automation jobs.	Malicious SQL can exfiltrate or corrupt all business data, create backdoor accounts, and destroy audit history. Breaks integrity of financials, customer records, and analytics, leading to compliance failures and downtime.	**High**

MinIO IAM Privilege Escalation	**Object Storage for Application Data & Backups (MinIO)**. Stores app artifacts, documents, and sometimes database backups and keys for multiple services.	Low-privilege user can become storage admin, read or delete any object, and plant backdoored data. Results in large-scale data breach, loss of backups, ransomware-style impact, and long recovery times.	**High**

Nist Family:

Risk Event (vulnerability)	**NIST Family**	**Family Code**	**Justification**
Payment Gateway Log Exposure	System and Information Integrity	SI	Primarily information-handling and integrity failure (SI-12 / SI-7). The system does not protect log contents or validate where logs are stored, allowing unauthorized disclosure of sensitive operational and customer data through exposed logs.
PureApplication Log Disclosure	Audit and Accountability	AU	Mapped to AU-9 (Protection of Audit Information). Log files containing credentials and configuration are readable by low-privilege users, meaning audit records and operational logs are not protected from unauthorized access or misuse.
Oracle Identity Manager Pre-Auth RCE	Access Control	AC	Core failure is AC-3 (Access Enforcement) and AC-6 (Least Privilege). The REST interface does not enforce authentication on all code paths, allowing unauthenticated users to reach a Groovy execution endpoint and obtain full administrative control.
PostgreSQL psql SQL Injection	System and Information Integrity	SI	This is an input-handling flaw aligned with SI-10 (Information Input Validation). The database interface fails to properly validate or constrain input passed into SQL statements, enabling injection that compromises data integrity and availability.
MinIO IAM Privilege Escalation	Access Control	AC	Maps to AC-2/AC-3 (Account Management and Access Enforcement). Weak IAM policy evaluation allows low-privilege identities to obtain admin-level permissions, breaking least-privilege and permitting unauthorized control over all stored objects.

R1 CVE-2023-38007: HTML Injection – IBM Cloud Pak System

Asset:
IBM Cloud Pak System – Web Management Interface

Vulnerability

HTML Injection due to Improper Input Sanitization

The web interface of IBM Cloud Pak System fails to properly sanitize user-supplied input, allowing attackers to inject malicious HTML content that is rendered by other users.

Assumptions

The attacker can trick a user into clicking or loading a malicious link

Input fields are not properly sanitized or encoded

Users authenticate through the vulnerable web interface

No Content Security Policy (CSP) is implemented

Initial Access

The attacker uses a low-privileged authenticated account to inject malicious HTML into an unsanitized input field within the Cloud Pak management interface.

Exploitation

The application renders the injected HTML without proper encoding, allowing the attacker to manipulate the user interface, display fake content, or trigger unintended actions.

Privilege Escalation

An administrator views the injected content, allowing the attacker to hijack the admin session or force unauthorized administrative actions through UI manipulation.

Remote Code Execution

With administrative access, the attacker abuses Cloud Pak management features to execute code within managed workloads or orchestrated services.

Lateral Movement

Compromised services enable movement across multiple Cloud Pak components, potentially leading to broader system compromise.

STRIDE Analysis

Tampering (T):
The attacker modifies page content and interface behavior through injected HTML.

Information Disclosure (I):
Malicious HTML can capture sensitive user data such as cookies, form inputs, or session tokens.

Likelihood: 3 / 5 (Moderate)

The attack requires user interaction and the presence of unsanitized input fields, which is realistic in exposed web management interfaces.

Impact: 4 / 5 (High)

Session hijacking or administrative compromise can expose sensitive workloads and configuration data.

Total Risk12 / 25 – Medium

DREAD Analysis

Category	Score	Reason
Damage	5	Primarily affects the user interface and user-level data
Reproducibility	6	Works reliably when input is not sanitized
Exploitability	5	Requires moderate technical skill
Affected Users	6	All users who load the malicious content
Discoverability	5	Requires probing and understanding of the interface

Final DREAD Score:5.4 – Medium Risk

R2 CVE-2017-12132: GNU glibc Memory Corruption Vulnerability

Asset:GNU C Library (glibc) – Core System Libraries

Vulnerability

Memory Corruption in GNU glibcA vulnerability in outdated versions of glibc allows attackers to trigger memory corruption, leading to arbitrary code execution, privilege escalation, and full system compromise.

Assumptions

The system runs an outdated version of glibc across multiple services

Attackers can execute code or trigger memory corruption conditions

Address Space Layout Randomization (ASLR) and modern exploit mitigations are disabled

glibc is used by nearly all system processes

Initial Access

The attacker gains access to a service running a vulnerable version of glibc, such as a network-facing or locally accessible process.

Exploitation

The attacker triggers a memory corruption flaw in glibc, exploiting unsafe memory handling within the library.

Remote Code Execution

The memory corruption allows the attacker to execute arbitrary native code on the affected system.

Privilege Escalation

The injected code executes with elevated operating system privileges, potentially granting root-level access.

Lateral Movement

With full system compromise, the attacker can pivot to other hosts, services, or network segments.

STRIDE Analysis

Tampering (T):
The attacker can modify process memory or inject malicious code.

Information Disclosure (I):
Memory leaks may expose sensitive information such as credentials or secrets.

Denial of Service (D):
Exploits can crash critical services or the operating system.

Elevation of Privilege (E):
Successful exploitation can lead to full system-level privilege escalation.

Likelihood: 4 / 5 (High)

The vulnerability is exploitable on outdated systems lacking ASLR and modern protections and affects many system processes.

Impact: 5 / 5 (Severe)

Successful exploitation results in full operating system compromise, privilege escalation, and lateral movement.

Total Risk 20 / 25 – Critical

DREAD Analysis

Category	Score	Reason
Damage	9	Privilege escalation enables full system control
Reproducibility	8	Public exploits exist and attacks are repeatable
Exploitability	9	Memory corruption vulnerabilities often have proof-of-concept code
Affected Users	10	glibc is used by nearly all system processes
Discoverability	8	The vulnerability is well-documented

Final DREAD Score:8.8 – Critical Risk

R3 Java SE Vulnerabilities – IBM Pure Application System

Asset: IBM Pure Application System – Java SE Runtime Environment (WebSphere / Application Servers)

Vulnerability

Unpatched Java SE Vulnerabilities Allowing Remote Code Execution

Unpatched Java SE runtimes in IBM Pure Application System allow attackers to exploit remotely triggerable flaws, leading to code execution, sandbox escape, and potential system compromise.

Assumptions

Java is heavily used across the platform (WebSphere and application servers)

Vulnerable Java SE runtimes are still present

Exploits can be triggered remotely through exposed application interfaces

No runtime patching, sandbox hardening, or additional JVM security controls are enabled

Initial Access

The attacker interacts with a Java-based service running on the IBM Pure Application System through exposed application interfaces.

Exploitation

The attacker exploits unpatched Java SE vulnerabilities, enabling code execution, or bypassing JVM sandbox restrictions.

Remote Code Execution

Malicious code executes within the Java Virtual Machine (JVM).

Privilege Escalation

The executed code runs with application-level or system-level privileges, depending on JVM and OS configuration.

Lateral Movement

The compromised JVM is used to access other platform services and components within the IBM Pure Application System.

STRIDE Analysis

Tampering (T):

Exploitation allows modification of application logic and runtime behavior.

Information Disclosure (I):

The attacker can access sensitive data stored or processed within Java applications.

Denial of Service (D):

The JVM or dependent applications may crash or become unavailable.

Elevation of Privilege (E):

Remote code execution may lead to full system or platform takeover.

Likelihood: 3 / 5 (Moderate)

Successful exploitation requires a vulnerable Java runtime and reachable interfaces; this is plausible but not guaranteed in all environments.

Impact: 4 / 5 (High)

A compromised JVM can affect multiple applications and critical platform services.

Total Risk12 / 25 – Medium

DREAD Analysis

Category	Score	Reason
Damage	9	Remote code execution can lead to full system compromise
Reproducibility	8	Exploits have been tested and demonstrated by researchers
Exploitability	7	Requires specific conditions and vulnerable runtimes
Affected Users	9	All Java-based components and users are impacted
Discoverability	8	Vulnerabilities are publicly disclosed

Final DREAD Score:8.2 – Critical Risk

R4) Weak Logging and Monitoring

Asset:Enterprise Systems – Logging, Monitoring, and Security Visibility Controls

Vulnerability

Insufficient Logging and Monitoring Controls

The system lacks centralized, complete, and protected logging, and does not implement effective monitoring, alerting, or anomaly detection. This allows attacker activity to remain undetected for extended periods.

Assumptions

Logs are incomplete, not centralized, or can be easily deleted or modified

No Security Information and Event Management (SIEM) alerts are configured

Anomaly detection and behavioral monitoring are absent

Critical security events are not monitored

Initial Access

The attacker gains limited or low-privileged access to the system through any initial compromise.

Exploitation

Insufficient logging and monitoring allow malicious actions to occur without detection or alerting.

Persistence

The attacker maintains long-term access to the environment without raising security alerts.

Privilege Escalation

Extended undetected access enables abuse of system misconfigurations or vulnerabilities to escalate privileges.

Lateral Movement

Without visibility or alerts, attacker activity spreads across systems and services.

STRIDE Analysis

Repudiation (R):
Weak logging prevents reliable attribution of malicious actions, enabling attackers to deny or conceal activity.

Likelihood: 3 / 5 (Moderate)

Incomplete logging and lack of monitoring are common in many environments, making attacker persistence moderately likely.

Impact: 3 / 5 (Moderate)

Undetected malicious activity allows continued access and attack chaining, increasing overall damage over time.

Total Risk9 / 25 – Medium–Low

DREAD Analysis

Category	Score	Reason
Damage	7	Incident detection and response become severely impaired
Reproducibility	9	Absence of logging is consistently exploitable
Exploitability	9	Requires only basic system access
Affected Users	6	Primarily impacts security operations and response teams
Discoverability	8	Weak logging controls are easy to identify

Final DREAD Score:7.8 – High Risk

R5 Outdated SSL/TLS Configuration

Asset: Enterprise Systems – Network Communications and Transport Security

Vulnerability

Support for Weak or Deprecated SSL/TLS Protocols and Ciphers

The system supports outdated SSL/TLS versions (e.g., TLS 1.0 / 1.1) and weak cryptographic ciphers, exposing sensitive data in transit to interception and manipulation.

Assumptions

The system supports weak or deprecated SSL/TLS protocols

Modern TLS standards (e.g., TLS 1.2 / 1.3) are not enforced

Sensitive data (credentials, session tokens, business data) is transmitted over the network

Initial Access

The attacker intercepts network traffic by exploiting weak or deprecated SSL/TLS protocols.

Exploitation

Insecure ciphers or protocols allow the attacker to decrypt traffic or perform man-in-the-middle (MITM) attacks.

Credential Compromise

Authentication credentials and session data are exposed and stolen during interception

Privilege Escalation

Stolen credentials are used to gain higher-level access to systems and services.

Lateral Movement

The attacker accesses additional services by abusing trusted connections and compromised credentials.

STRIDE Analysis

Information Disclosure (I):
Weak SSL/TLS configurations allow eavesdropping on sensitive communications.

Tampering (T):
MITM attacks enable modification of data in transit.

Likelihood: 3 / 5 (Moderate)

Exploitation is possible when weak ciphers or outdated protocols remain enabled.

Impact: 4 / 5 (High)

Exposure of credentials or sensitive data can lead to account compromise and further attacks.

Total Risk12 / 25 – Medium

DREAD Analysis

Category	Score	Reason
Damage	7	Sensitive data can be intercepted or altered
Reproducibility	8	MITM attacks are repeatable when weak TLS is present
Exploitability	7	Widely available tools; moderate skill required
Affected Users	8	All clients communicating with the server
Discoverability	9	Weak ciphers and protocols are easy to identify

Final DREAD Score:7.8 – High Risk

Threat Propagation Matrix:

#	Vulnerability / Asset	Entry Point	Primary Impact	Propagation Path	Final Impact
1	Web UI – HTML Injection	Web application interface	Session hijacking	Injected HTML steals session tokens → attacker impersonates users	Partial interface compromise
2	glibc Library	Service using vulnerable glibc	Memory corruption	Exploited process → OS-level privilege escalation	Full system compromise

3	Java Runtime (JVM)	Java-based application / API	JVM exploitation	JVM compromise → access to system APIs and resources	Critical system compromise
4	Logging System	Logging / monitoring interface	Activity not recorded	Attacks go undetected → attacker chains multiple attacks	Persistent compromise
5	TLS Layer	Network communication channel	Data interception	Stolen credentials → unauthorized logins	High-impact data exposure

Contextual Risk Register:

Risk Event	Context (Asset/Process)	Business Impact	Real Score
1) HTML Injection – IBM Cloud Pak System (CVE-2023-38007)	**IBM Cloud Pak System Web UI** – the hybrid cloud management platform that hosts multiple workloads and interfaces.	Attacker injects malicious HTML → session hijacking and admin takeover → exploit management functions → remote code execution inside managed workloads → lateral movement across Cloud Pak components.	Medium
2) GNU glibc Vulnerabilities (CVE-2017-12132)	**Services running on outdated glibc within IBM OS Images / Containerized services** – glibc is a core library used by most Linux-based processes including Cloud Pak infrastructure services.	Memory corruption → OS-level privilege escalation → full system compromise → lateral spread to other hosts and services.	Critical

3) Java SE Vulnerabilities – IBM PureApplication System / JVM runtimes	**IBM PureApplication System and Java-based workloads** – Java runtimes for app servers that host business logic, APIs, and internal services.	Unpatched Java SE flaws → remote code execution in JVM → privilege escalation and full system takeover → lateral movement to other platform services.	Critical
4) Weak Logging / Monitoring	**Logging & monitoring across Cloud Pak / WAS / Kibana dashboards** – central logs for audit trails and security alerts (e.g., WAS log streams and Kibana log dashboards for Cloud Pak).	Logs incomplete or not monitored → malicious actions go undetected → attacker persistence and unobserved privilege escalation → lateral movement.	High
5) Outdated SSL/TLS Configuration	**TLS/SSL communications in IBM DataPower Gateway and Cloud Pak network interfaces** – TLS used for encrypted data in motion between clients, APIs, and backend services.	Weak ciphers or deprecated protocols → encrypted traffic can be intercepted or downgraded → credentials/tokens compromised → unauthorized access and lateral movement.	High

Nist Family:

Risk Event (Vulnerability)	**NIST Family**	**Family Code**	**Justification**
Improper Access Control (RCE) – IBM Cloud Pak System (HTML Injection, CVE-2023-38007)	Access Control	**AC**	The core failure is access enforcement: the application does not sanitize user input, allowing unauthorized HTML that leads to session compromise and further unauthorized actions — a violation of AC-3 (Access Enforcement).

GNU glibc Vulnerabilities (Memory Corruption / Privilege Escalation)	System and Information Integrity	**SI**	Root cause is memory corruption affecting core runtime libraries, a failure in integrity of process memory and control flow. This represents a systemic integrity failure (SI-7: Software, Firmware, and Information Integrity).
Java SE Vulnerabilities – Java Runtime in IBM PureApplication System	System and Information Integrity	**SI**	Vulnerable Java runtimes allow arbitrary code execution and integrity breaches in hosted applications, representing unreliable input handling and integrity failures (SI-7).
Weak Logging / Monitoring	Audit and Accountability	**AU**	Logging failures and missing monitoring directly impact accountability — failure to protect audit records and generate reliable event logs (AU-2, AU-9).
Outdated SSL/TLS Configuration – IBM DataPower Gateway	System and Communications Protection	**SC**	Use of weak or obsolete cryptography affects cryptographic protection of data in transit, violating SC-8 (Transmission Confidentiality) and SC-13 (Cryptographic Protection).

IBM Compliance

IBM Cloud uses NIST standards. Link

Control ID	Control Name	IBM Cloud Implementation	Gaps / Weaknesses	Score
AC-02	Account Management	IBM Cloud IAM manages user accounts, service IDs, and access roles.	Improper account lifecycle management by customers may lead to risks.	9
AT-02	Security Awareness and Training	IBM Cloud provides security training materials, short courses, and official videos.	Effectiveness depends on user participation.	10
AU-02	Event Logging	IBM Cloud Activity Logs capture resource actions and administrative events.	Log retention settings can be modified by privileged users.	6
CA-02	Security Assessments	IBM Cloud performs regular security assessments and compliance audits.	Limited assessment detail visibility for customers.	8
CM-02	Baseline Configuration	IBM Cloud maintains secure baseline configurations for infrastructure and services.	Customer misconfiguration remains a shared responsibility risk.	8
CP-02	Contingency Planning	IBM Cloud supports backup, recovery services, and availability zones.	Customers must design and test recovery plans themselves.	9
IA-02	Identification and Authentication	IBM Cloud enforces authentication via IAM, MFA, and identity federation.	Weak customer password policies may reduce effectiveness.	9
IR-02	Incident Response Training	IBM Cloud has internal incident response processes and response teams.	Customers must conduct their own response training.	8
MA-02	Controlled Maintenance	IBM Cloud performs scheduled and emergency maintenance securely.	Maintenance transparency is limited to notifications.	8

MP-02	**Media Access**	**IBM Cloud controls access to storage media within data centers.**	**Customers have limited visibility of media handling.**	**9**
PE-02	**Physical Access Control**	**IBM Cloud data centers use strong physical security controls.**	**Customers cannot directly verify controls.**	**10**
PL-02	**System Security Plan**	**IBM Cloud documents security architecture and shared responsibility models.**	**Customers must maintain their own system plans.**	**8**
PM-02	**INFORMATION SECURITY PROGRAM LEADERSHIP ROLE**	IBM Cloud defines clear **Leadership Roles** and responsibilities for **CISO** and the GRC team.	**Customers** must define and assign their own **Security Lead** role for their cloud environment oversight.	**9**
PS-02	**Personnel Screening**	**IBM Cloud screens employees with access to sensitive systems.**	**Screening details are not fully disclosed.**	**9**
RA-02	**Risk Assessment**	**IBM Cloud conducts continuous risk assessments across services.**	**Customer-specific risks are customer-managed.**	**8**
SA-02	**System Development Lifecycle**	**IBM Cloud integrates security throughout the system development lifecycle, including secure design, development, testing, and deployment processes**	**None identified.**	**10**
SC-02	**Application Partitioning**	**IBM Cloud uses virtualization and container isolation techniques.**	**Misconfigured workloads may weaken isolation.**	**8**
SI-02	**Flaw Remediation**	**IBM Cloud applies patches and vulnerability fixes regularly.**	**Customers must patch guest OS and applications.**	**8**
SR-02	**Supply Chain Risk Management**	**IBM Cloud manages vendor and supply chain risks.**	**Supply chain transparency is limited.**	**7**
PT-02	**PII Processing and Transparency**	**IBM Cloud provides data protection and privacy controls.**	**Customers control most PII handling.**	**8**

Critical Thinking

If the Payments Database is attacked:

1. If it's DOWN for 24 hours:

- All money transfers STOP
- No one can see if payments worked
- Banks get big fines immediately
- Companies won't know who paid them

2. If it's HACKED (someone gets in):

- FIRST: Thieves can change where money goes (send it to their accounts)
- SECOND: They steal all customer payment details
- THIRD: Banks must pay huge fines + pay back stolen money + lose customer trust

3.Reaching the crown jewel data

- Enter payment system - now sees all money movements
- From there, can reach:
  - Money transfer systems → Steal cash
  - Customer database → Steal all personal data
  - Admin controls → Take over bank operations

Monitoring the system

1. If Monitoring/Logging is DOWN for 24 Hours:

- Complete Attack Blindness: We cannot detect ongoing attacks in real-time
- No Forensic Evidence: If an attack happened, we cannot investigate or track it
- Compliance Violation: Many regulations (GDPR, PCI DSS, SOX) require logging which can leads to fines

2. If Monitoring/Logging is HACKED:

- Attacker Gains Full Visibility: They can see all user logins, API calls, and system events
- Credential Theft: Can capture usernames, passwords, session tokens from logs
- Learn Business Patterns: Study how admins operate, when backups run, what normal traffic looks like
- Evade Future Detection: Delete or alter logs to cover their tracks forever

3. Path to Crown Jewels via Compromised Logging:

- Hack logging system
- See admin login patterns
- Capture admin credentials
- Wait for right moment
- Use stolen creds to access crown jewel systems
- Delete all evidence of attack

Object storage

1. If Object Storage is DOWN for 24 Hours:

- Users can't access their files (photos, documents, backups)
- Critical applications fail if they need stored data to run
- Bad reputation and potential contract violations
- Could stop disaster recovery if backups are stored here

2. If Object Storage is HACKED:

- Mass Data Leak: All stored files exposed (photos, documents, database backups)
- Ransomware Attack: Encrypt everything and demand payment
- Compliance Disaster: Violates GDPR, HIPAA, PCI DSS (huge fines)
- Supply Chain Attack: Malicious files can be swapped in, infecting anyone who downloads them

3. Path to Crown Jewels via Object Storage

- Get into object storage
- Find database backups
- Download and restore backup files
- Extract sensitive data (logins, payments, PII)
- OR: Replace clean files with infected versions
- Wait for systems to use infected files

IBM PureApplication (Session/Transaction Data)

1. If IBM PureApplication is DOWN for 24 Hours:

   - **Statelessness:** If session data is lost, users get logged out repeatedly.
   - **Audit Failure:** If transaction data logs are not being written, the business loses the "proof" of transactions occurring during this window, leading to potential legal disputes with partners.

2. If IBM PureApplication is HACKED:

   - **Session Hijacking:** If an attacker can manipulate the session store, they can clone valid user sessions.
   - **Privilege Escalation:** By modifying session objects directly in the store, an attacker could change flags without needing a password.

3. Path to Crown Jewels via IBM PureApplication:

   - Gain Access to the Session Store
   - Locate Admin Session Tokens
   - Modify or Inject a New Privileged Session
   - Use the valid admin Session for Impersonation
   - Access admins account

IAM Data Store (User Credentials)

1. If IAM Data Store is DOWN for 24 Hours:

- Users cannot log in to any system or application
- All authentication-dependent services fail (apps, APIs, cloud consoles)
- Administrators cannot manage users, roles, or permissions
- Business operations stop due to complete access lockout
- Severe reputation damage and possible SLA / contract violations

2. If IAM Data Store is HACKED:

- Credential Theft: Usernames, passwords, tokens, and keys are stolen
- Account Takeover: Attackers impersonate users and administrators
- Privilege Escalation: Compromised admin accounts give full system control
- Compliance Disaster: Violates GDPR, ISO 27001, SOC 2 (massive penalties)
- Persistent Access: Attackers create hidden accounts or backdoors

3. Path to Crown Jewels via IAM Data Store:

- Gain access to IAM data store
- Steal admin credentials or authentication tokens
- Log in as privileged users
- Access critical systems (databases, object storage, cloud workloads)
- Disable security controls and logging
- Extract sensitive data (PII, financial data, intellectual property)

Credential Theft Chain Intersection:

Intersection point 1

Cascade Path:

- WebSphere response splitting → XSS → cookie theft
- ONNX path traversal → reading files that contain credentials
- DataPower weak TLS → intercepting and decrypting tokens
- Cloud Pak RCE → using the stolen credentials for deeper system access

Result:

A full attack chain that leads to **all system compromise** by combining multiple simple vulnerabilities.

Intersection point 2: HTML Injection + Weak Logging + Java Runtime

Intersection Components:

- Web UI HTML Injection
- Weak Logging
- Java SE Vulnerabilities

Combined Threat:

Session hijacking + invisible exploitation

Cascade Path:

- HTML injection steals admin session cookies
- Attacker accesses Java admin interfaces
- Exploits unpatched Java runtime for RCE
- Weak logging prevents detection of privilege abuse

Intersection point 3: Monitoring Failure + Incident Response Gaps

Risks:

- Incomplete monitoring
- Weak alerting
- Insufficient incident response training

Cascade Path:

- Initial attack goes unnoticed
- No alerts trigger investigation
- Attackers establish persistence
- Multiple systems are compromised over time

Most Severe Risks (Critical)

The following risks are classified as the **most severe** because they combine **high likelihood** with **severe impact**, leading to **remote code execution, full system compromise, and lateral movement** across the environment. Immediate remediation is required to prevent catastrophic security breaches.

R2 – CVE-2017-12132 (GNU glibc Memory Corruption)

Why this is a severe risk

glibc is a core system library used by nearly all processes. Exploitation enables **OS-level privilege escalation and full system takeover**, making all other security controls ineffective.

Why remediation is needed

Failure to fix this vulnerability exposes the entire operating system to compromise and allows attackers to pivot to other systems.

How to remediate

- Upgrade glibc to a patched version
- Enable ASLR and exploit mitigations
- Apply OS hardening and least privilege

Y5 – CVE-2025-3357 (IBM Tivoli Monitoring RCE)

Why this is a severe risk

The vulnerability allows **remote code execution without user interaction** in a trusted monitoring system, enabling attackers to control monitored hosts and hide malicious activity.

Why remediation is needed

A compromised monitoring system undermines visibility, detection, and trust across the entire infrastructure.

How to remediate

- Apply IBM security patches
- Restrict network access to monitoring services
- Enforce input validation and strong logging

M1 – CVE-2025-48734 (IBM Cloud Pak System – Improper Access Control)

Why this is a severe risk

Exploitation leads to **full JVM remote code execution**, allowing attackers to compromise Cloud Pak services and move laterally across platform components.

Why remediation is needed

Cloud Pak is a central orchestration platform; compromise impacts multiple applications and business services simultaneously.

How to remediate

- Patch Cloud Pak and Apache Commons BeanUtils
- Restrict ClassLoader and reflection access
- Enforce least privilege for JVM services

J3 – CVE-2025-61757: Oracle Identity Manager Pre-Authentication RCE (CRITICAL)

Why this is a critical risk

This vulnerability allows a **completely unauthenticated attacker** to achieve **full remote code execution** on Oracle Identity Manager by bypassing authentication controls using crafted WADL/WSDL metadata suffixes. Because OIM is the **central IAM authority**, exploitation results in **total identity infrastructure compromise**, enabling attackers to impersonate users, create privileged accounts, revoke tokens, and control authentication across all connected systems.

Why remediation is mandatory

Oracle Identity Manager is a crown-jewel system. Compromise does not affect a single application—it collapses trust across the entire enterprise. With confirmed active exploitation (CISA KEV) and public proof-of-concepts, failure to remediate exposes millions of users, violates regulatory obligations (GDPR, PCI DSS, SOX), and enables business-ending outcomes such as total service shutdown, fraud, and irreversible reputational damage.

How to remediate

- Immediately patch Oracle Identity Manager and underlying WebLogic to vendor-fixed versions
- Block metadata suffixes (;.wadl, ?WSDL, similar) at WAF, reverse proxy, and application layers
- Disable or strictly restrict Groovy script execution endpoints
- Enforce network isolation for IAM services (no direct internet exposure)
- Rotate all credentials, tokens, API keys, and secrets managed by OIM after patching
- Enable enhanced logging and real-time alerting for IAM administrative actions
- Conduct a full compromise assessment to identify persistence mechanisms or backdoor accounts

M2 – Path Traversal Vulnerability (IBM Watson Speech Services Cartridge for IBM Cloud Pak for Data)
(CVE referenced via IBM Advisory: 7162199)

Why this is a severe risk

The vulnerability allows **unauthenticated remote attackers** to perform path traversal via the exposed ONNX endpoint. Successful exploitation enables **arbitrary file read access**, potentially exposing configuration files, credentials, logs, or model data. Stolen credentials can be reused for **privilege escalation and lateral movement** within the Cloud Pak environment.

Why remediation is needed

IBM Watson Speech Services is commonly deployed as part of **data processing and AI pipelines**. Exposure of internal files or secrets can compromise not only the cartridge itself but also **dependent services, APIs, and integrated platforms**, increasing the blast radius of the attack.

How to remediate

- Apply IBM patches addressing the ONNX path traversal vulnerability
- Enforce strict input validation and canonical path checks on ONNX endpoints
- Restrict filesystem access permissions for the Watson Speech service
- Store credentials and secrets outside readable filesystem paths

Realistic Constraints of IBM Cloud

1. Shared Responsibility Model

IBM Cloud secures the underlying infrastructure, but **customers are responsible for configuration, identity management, patching guest OSs, and application security**. Misconfigurations on the customer side cannot be fully prevented by IBM

2. Availability and Uptime Requirements

Many IBM Cloud customers operate **mission-critical systems** (banking, healthcare, government):

- Downtime is unacceptable
- Security patches may be delayed to avoid service disruption
- Emergency fixes require extensive testing

3. Supply Chain and Third-Party Dependencies

IBM Cloud services depend on:

- Open-source components
- Third-party vendors
- Acquired platforms (e.g., SoftLayer legacy infrastructure)
  Customers must **trust IBM's vendor risk management**, reducing direct control.

4. Regulatory and Compliance Constraints

IBM Cloud must support **multiple global regulations** (GDPR, HIPAA, PCI DSS, ISO 27001,NIST):

- Security controls must balance compliance and usability
- Some regions restrict data movement or logging practices

5. Scale and Multi-Tenancy

IBM Cloud operates at **massive scale with multi-tenant environments**:

- Security controls must avoid impacting other tenants
- Aggressive monitoring or isolation may introduce performance overhead