Top Threats to Cloud Computing:
Egregious Eleven Deep Dive

First Look: Capital One (SSRF Attack 2019)

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal Less Experienced Cloud Architects, Less Experienced Solutions Architect	**Shared Technology Vulnerabilities** - Exposure of AWS cloud platform SSRF vulnerability	**EE8** **Weak Control Plane** - AWS allows meta data interrogation	**EE 1** **Data Breach** - Resulting in PII from 106M consumer credit applications	**Financial** - $150M Notification (est) - 6.9% Capital One stock price drop - Possible regulatory fines	**Preventative** - DSI-02 - GRM-01 - IAM-02 - IVS-13 - SEF-01
	Abuse and Nefarious Use of Cloud Services - VPN and anonymous network services used to manipulate identity	**EE 2** **Misconfiguration and Inadequate Change Control** - ModSecurity Web Application Firewall allowed Server-Side Request Forgery (SSRF)	**EE9** **Metastructure and Applistructure Failures**- default hypervisor trust allows service discovery and interrogation	**Operational** - Incident Response - Forensics Analysis - Informing affected parties	**Detective** - CCC-03 - GRM-02 - IAM-13 - IVS-01
External Former CSP Trusted Insider	**Complicated Environment** - Intimate knowledge requirements for correct implementation and configuration decisions	**EE4** **Insufficient Identity & Credential Management** - over provisioned EC2 and S3 roles for WAF and storage	**EE11** **Abuse & Nefarious Use of Cloud Services:** former AWS administrator with intimate knowledge of AWS operations	**Compliance** - Sensitive Data Leakage - Class Action Lawsuits -Congressional Inquiry **Reputational** - Cloud (CSP) Loss of Confidence - Long term stock price	**Corrective** - HRS-09 - IAM-07 - IVS-06 - SEF-02 - SEF-03 - SEF-04 - TVM-02

Attack Detail

Actor: Former engineer of AWS with insider knowledge on platform vulnerabilities gained credentials from a misconfigured web application to extract sensitive information from protected cloud folders

Attack: Open-source anonymity network (Tor) and VPN services (iPredator) hides attacker. Misconfigured ModSecurity WAF used by Capital One with their AWS cloud operations relayed AWS cloud metadata services including credentials to cloud instances. Over privileged access given to the WAF allowed the attacker to gain access to multiple protected cloud folders (AWS S3 buckets) with the ability to read data sync and exfiltrate sensitive information.

Vulnerabilities: A Server Side Request Forgery (SSRF) vulnerability on the platform was exposed in which a server (e.g. Capital One's WAF) was tricked into requests from an attacker to access cloud server configurations (e.g. EC2 metadata service) including credentials to whatever the server had access to.

Technical Impacts

Data Breach: A web application was compromised for IAM credentials to access multiple cloud folders. The cloud folders accessed had read rights to 106 million records of customer information that were exfiltrated.

Data Loss: The data extracted were credit card applications and credit card customer status reports between 2005-2019. Personal Identified Information (PII) from the applications included applicant names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. The credit card customer PII and financial records extracted included credit scores, credit limits, balances, payment history, contact information, social security numbers, and linked bank accounts. Approximately 140,000 Social Security numbers and 80,000 linked bank account numbers of secured credit card customers were exfiltrated.

Business Impacts

Financial: The exposure of customer bank account information can lead to loss of customer financials and insurance costs for the banking institution. Impact on 106 million customers will lead to a settlement estimated between $100-500M for customer credit monitoring, identity restoration services, fraud, or other misuse of customer information. Additional regulatory violations will lead to fines up to $500M. The increase in penalties paid and loss of revenue will lead stock prices to fall.

Operational: Incident response and additional legal investigation; replaement and retraining of security staff; risk and vulnerability assessments and reconfigurations of applications; and notifications to customers and repairing of damage disrupted normal business operations

Compliance: Loss of customer PII leads to violations with GDPR and other privacy regulations leading to monetary penalties. Higher regulated industries such as the finance services puts financial institutions under strict monitoring for customer protection with heavy penalties. Equifax faced $575M in fines from the US Federal Trade Commission in a data breach in 2017 that impacted 147 million customers.

Reputational: The loss of customer and applicant information is expected to impact Capital One customer and public confidence with revenue decreases expected over the three years following the incident due to fewer customer acquisitions. The breach also had reputational losses internally with the CISO being reassigned and almost a dozen security professionals at the organization quitting.

Prevention Mitigation

DSI-02: *Data Inventory Flows*
Inventory, documentation, and maintenance of data flows will identify and establish the secure archiving, destruction, and disposal of aging customer data.
GRM-01: *Baseline Requirements*
Established security requirements will prevent deviations from baseline configurations and identify vulnerabilities before implementation and use of an application.
IAM-02: *Credential Lifecycle / Provision Management*
Appropriate policies, procedures, processes and measures will prevent the over-provisioning of access to excessive cloud folders and sensitive information.
IVS-13: *Network Architecture*
Architecture diagrams and data flows are applied for timely detection and response to network penetration and the exfiltration of data.
SEF-01: *Contact Authority Maintenance*
Points of contact for regulators and law enforcement are maintained for immediate compliance and preparation for forensic investigation when a breach occurs.

Detective Mitigation

CCC-03: *Quality Testing*
Quality change control and testing is established for application misconfigurations affecting the confidentiality, integrity, and availability of the systems and services.
GRM-02: *Data Focus Risk Assessments*
Data focused assessments discover the proper and improper use, storage, destruction, and access of sensitive data.
IAM-13: *Utility Programs Access*
Identify the AWS server vulnerability to an SSRF attack and restrict the IMDS metadata exploit. (AWS IMDSv2 has since fixed the occurrence of this type of SSRF attack.)
IVS-01: *Audit Logging/Intrusion Detection*
Proper log management for suspicious network behaviors and file integrity anomalies are recorded for investigation in the event of a security breach.

Corrective Mitigation

HRS-09: *Training / Awareness:*
Cloud architecture and data lifecycle management will identify misconfigurations, over-permissioned applications, and improper data management processes. Continuous training on cloud platforms and security techniques prepares staff for recent platform features and the latest types of attacks.
IAM-07: *Third Party Access*
Assessment of risks posed by third party access to cloud services will identify over-permissioned and other inappropriate access by a WAF or other applications.
IVS-06: *Network Security*
Implement the latest design and configuration techniques to monitor access and behavior from trusted and untrusted connections.
SEF-02: *Incident Management*, **SEF-03:** *Incident Reporting*, **SEF-04:** *Legal Preparation*
Response to an incident, breach notification, and forensics procedures will be conducted in a timely manner with impacted customers, third parties, regulatory bodies, and other legally required entities.
TVM-02: *Vulnerability/Patch Management*
Identify vulnerabilities such as SSRF in the IMDS platform and patch or push for a CSP patch.

Metrics

Key Performance Indicators: Misconfiguration scans, cloud architecture expertise, data inventory model, credential provisioning

Control Effectiveness Measurements: Implementation architecture and data flow diagrams, data storage and disposal archiving, access control alerting

Key Takeaways

- Misconfigured applications can compromise cloud server metadata exposing storage folders.
- Over-permissioned cloud apps allow access to too much data when compromised.
- Data inventory/lifecycle practices archives, destroys, and disposes data limiting exposure.

References

Capital One breach details

1. https://cloudsecurityalliance.org/blog/2019/10/10/cloud-penetration-testing-the-capital-one-breach/
2. https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach/
3. https://www.capitalone.com/facts2019/
4. https://www.scmagazine.com/home/security-news/capital-one-breach-exposes-not-just-data-but-dangers-of-cloud-misconfigurations/
5. https://krebsonsecurity.com/tag/capital-one-breach/
6. https://krebsonsecurity.com/tag/paige-a-thompson/
7. http://web.mit.edu/smadnick/www/wp/2020-07.pdf

SSRF

8. https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SS

Estimated cost of Capital One breach

9. https://fortune.com/2019/07/31/capital-one-data-breach-2019-paige-thompson-settlement/
10. https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/#f-2faa4437b79

Job loss at Capital One

11. https://www.bankinfosecurity.com/following-massive-breach-capital-one-replacing-ciso-report-a-13385

Equifax breach penalties

12. https://techcrunch.com/2019/07/22/equifax-fine-ftc/#:~:text=FTC%20slaps%20Equifax%20with%20a%20fine%20of%20up,M%20for%202017%20data%20breach&text=Credit%20agency%20Equifax%20will%20pay,a%20data%20breach%20in%202017.

Definitions

EC2 - Amazon Elastic Compute Cloud
GDPR - European Union General Data Protection Regulation
S3 - Amazon Simple Storage Service
SSRF - Server Side Request Forgery
VPN - Virtual Private Network
WAF - Web Application Firewall