Study on Risk and Impact of Source Code Leakage from Software Vendors

April 2021

CONTENTS

1. SUMMARY

A number of IT security incidents have been reported recently on software vendors who provide software and services to the financial industry. Security breaches that result in leakage or theft of source codes for applications supporting the financial institutions' ("FIs") critical functions and may have a material impact to the business operations and customers.

A workgroup was formed to look into a whitepaper to understand the risk and impact of source code leakage from third parties and to propose controls to strengthen protection and monitoring of source codes to minimise the likelihood of such events. In addition, this whitepaper will explore how the FIs should prepare and respond in the event of such security incidents.

FIs are recommended to assess the controls related to source code repositories in the third party service providers prior to commencement of service, and establishing an incident response and management plan to manage incidents of source code leakage or thefts. This includes assessing its impact, taking immediate actions to ensure integrity of the critical applications and infrastructure, and implementing measures to address the root cause.

2. INTRODUCTION

2.1 Definition of Source Code

For the purposes of this white paper, we elaborate on NIST's definition of "source code[1]". Source code includes program text, configuration files and other resources that are collectively used to generate software. Since libraries and binaries are compiled from source code, the users of such runtime library or binary may not have access to the original source code. If the library contains sensitive code, then the source code leakage controls would apply to the owners of the source code used to generate the library.

2.2 Threat Scenarios for Source Code Leakage

The risk to the FIs arising from the leakage of source code would be the highest if software that is critical to the operations of the FI were to be compromised. The following is a non-exhaustive list of third parties where incidents of source code leakage or theft may have the greatest impact to an FI:

- Fintech companies or software development companies who develop customised software used by FIs (known as "outsourced software vendor" for the purpose of the paper);
- Software development companies who develop commercial off-the-shelf ("COTS") products that are used by the FIs (known as "COTS software vendor" for the purpose of the paper);
- Outsourced service providers providing SaaS, PaaS or IaaS environments; or
- Organisations that develop critical applications and infrastructure used by the FI (e.g., ATM software, payment processing applications).

Third parties (referring to both "outsourced software vendor" and "COTS software vendor") may share source code with other organisations for specific purposes, for example, to perform source code reviews/ethical hacks to identify vulnerabilities or for escrow and archival. FIs should be cognizant of these potential avenues for leakage. At a high level, scenarios that could potentially lead to software theft or leakage are summarised below:

[1] NIST Source Code definition: https://samate.nist.gov/BF/Enlightenment/Definitions.html#:~:text=Source%20Code,design%2C%20implementation%2C%20or%20operation.

Theft or Malicious insider	Employees of the software development organisation who have access to the sensitive source code may deliberately steal or disclose this to unauthorised individuals, for a variety of motives including financial gain.
Accidental or unauthorised disclosure to outsiders	Sensitive code may be accidentally disclosed to unauthorised outsiders through misconfiguration of source code repositories, errors in access control setup etc.
Outcome of a successful cyber attack	Cyber criminals, nation states or other threat actors may exploit a combination of existing vulnerabilities in the vendor or third party's environment and/or social engineering techniques to gain access to sensitive source code. The controls on a third party software development organisation may be less sophisticated than the controls present in a FI.

2.3 Risk and Impact of Source Code Leakage

FIs could be at risk if the attackers or unauthorised entity in possession of the source code analyse the code to:

- Identify security controls including validations and checks embedded in the code, which could be used to craft attacks that can bypass these controls;
- Obtain proprietary logic or algorithms embedded in the code, which may result in loss of intellectual property or competitive advantage of the organisation; or
- Identify unknown vulnerabilities that may be exploited for targeted attacks.

This could cause a huge impact to FIs, in terms of data breaches, financial losses and reputational consequences.

A number of source code leakage incident[2] have been reported where attackers exploited vulnerabilities and insecure configurations to access networks and steal source code repositories from government agencies and private businesses. In one instance, attackers published the stolen source codes on a self-hosted public repository and stole data, an impacting the FIs and their clients.

3. CONTROLS

This section details about recommended technical and non-technical controls to prevent source code leakage. The controls for addressing the risks of source code leakage should be applied, at a minimum, to all sensitive code and all instances where they may be stored.

3.1 Identification of Sensitive Source Code

Identification of sensitive source code is a pre-requisite for implementing controls for prevention of source code leaks as well as determining the response to a suspected / confirmed source code leakage incident. The owners of the source code are responsible for completing this activity. The following are the guidelines for the FIs (in case of outsourced software development) and third parties (for e.g., COTS software providers) on identifying sensitive source code:

- Code is considered to be sensitive if the possession of the specific code can be leveraged by an unauthorised entity to cause financial or reputational loss. Examples of sensitive code include codes that contains proprietary processing logic, protected intellectual property, security

[2] Examples of notable recent source code leakage incidents are listed in the Appendix, Section 5.2.

configurations etc. For example, these may relate to payment systems, trading applications and ATM software that are used by the FIs.

- Each organisation should define their criteria for the identification of sensitive code and apply it to the inventory of code they possess.
- Third parties should conduct a holistic assessment to analyse their code inventory and identify all instances of code that is considered sensitive.
- Third parties should consider automated code scanning to detect and block codes with credentials and cryptographic keys from being added to the code repository by developers.

3.2 Assessment of Control Environment

Outsourced software vendor

When using an outsourced software vendor, it is important to ensure that the outsourced activity is properly managed and appropriate due diligence is conducted on the software vendor to ascertain that they have implemented the basic controls including:

- Having adopted an industry standard general information security management and controls framework, e.g. industry certifications such as ISO27001 or shared standardised assessments;
- Having implemented standard security controls and can demonstrate ongoing compliance, for e.g., via regular scanning, entitlement reviews, etc;
- Providing ongoing user education on information security topics including phishing & social engineering threats and actions to be taken to prevent it;
- Scanning of out-going mails, file uploads for sensitive content including source code; and
- Establishing effective end-point controls at a minimum to detect and remove malicious and unwanted software from end points that may be used to access sensitive code.

COTS software vendor

Instead of developing software in-house or via an outsourced vendor, FIs may choose to acquire well known or widely available COTS software. However, given that COTS software is more widely available and used in the industry, this makes COTS software attractive as a point of attack for hackers to have far-reaching impact across the industry. FIs need to understand that this risk and build security considerations into the COTS software acquisition process:

- Connection of COTS software with other systems in FIs: FIs should understand how are purchased COTS software connected to other systems, to help identify vulnerabilities that could be exploited and possibly impacting other systems' functionality.
- *Type of information stored within COTS software:* Depending on the type of data housed within the COTS software, this will help to determine the acceptable level of risks for each specific COTS software.
- *Audit:* FIs should consider whether the COTS software vendor allows for an independent audit / certification of their software and development process.
- *Reputation of COTS software vendor:* The reputation and credentials of the COTS software vendor should be assessed.
- *Notification mechanisms to the FIs:* FIs should consider whether the vendor has put in place notification mechanisms to the FIs in the event of any material events.
- *Delivery and support services by COTS software vendors:* FIs should consider the delivery and support services offered by the COTS software vendors.

Despite best efforts to assess the control environment of third parties, there may still be a risk of attack and loss of data. Third parties should consider implementing data loss prevention ("DLP") controls within

their internal environment to monitor possible source code leakage channels, e.g. via emails, uploads to cloud storage platforms, use of portable storage on:

- Data in use at endpoints, e.g. developers' PC and application development; and
- Data at rest in storage, e.g. source code repositories and escrows agents housing the source codes.

3.2 Contractual Obligations

Outsourced software vendor

After performing appropriate due diligence on the outsourced software vendor, the FI shall outline an outsourcing agreement to govern the relationships, obligations, responsibilities, rights and expectations of both parties. A FI may have regulatory obligations or timeline to meet (e.g. MAS Notice 644 to notify regulatory authorities not later than 1 hour, upon the discovery of a relevant incident) and when the incident relates to a third party vendor, it becomes imperative for FI to rely on the vendor's timely notification as well as cooperation to determine the impact and outcome of the incident. As a result, the following should be outlined in the agreement for vendors to protect the interests and rights of FI:

- Notification to the financial institution on a timely basis, when the vendor becomes aware of any security incidents related to source code leakage. FIs should ensure that any designated escalation line is clearly communicated to the vendor. Where there are stipulated regulatory timelines for reporting, these should be clearly defined in the agreements as well.
- Notification to the financial institution on any suspected or actual infringement of any Intellectual Property ("IP").
- Performing a root cause and impact analysis for incidents involving the financial institutions' software and data
- Cooperating in good faith and aiding the financial institutions where reasonably requested.

COTS software vendor

FIs are bounded by the terms and conditions set out in the End User or Master Software Agreement. As highlighted in Section 3.1 of the paper, FIs should assess the criticality of information stored within the COTS software, ability of vendor to notify material events, risks and impact of leakage to determine if the contract satisfies the minimum requirements set out by the FIs.

3.3 Access Control and Management

Regardless of how the code was acquired, the third parties in possession of the source code should have a complete, accurate and up-to-date inventory of source code. The objective of access control and management is to ensure that only authorised access is allowed to the source code repository and the access is limited to the segments of code that are required to complete the activity.

There are many use cases where source code can be accessed. Access to code may include, but is not limited to:

- Developers, reviewers etc. accessing the code on-demand using interactive IDEs, version control software etc., as part of their job function; and
- Access to the repository by automated tools for schedule activities such as unattended compilation / build, source code vulnerability scans etc.

Automated tools may have privileged access to the entire repository. Hence, it is imperative to configure the tools to ensure their access is secured and auditing the activities performed by the tools are implemented.

Below are the recommended best practices to ensure that access control and management is defined and managed in a consistent and timely manner. Where source codes are identified to be sensitive, FIs and third parties are highly encouraged to ensure that these practices are put in place.

Financial Institutions

- If sensitive source codes owned by the FI is managed by third parties, for e.g., Github, then the FI should consider managing such sensitive repositories internally and/or to segregate them from other less sensitive repositories.
- FIs should ensure adequate access controls and monitoring is implemented for access to the sensitive source code.
- Upon termination of contract, the third party access to sensitive code should be removed, and/or sensitive code repositories on third parties should be irrevocably deleted.
- When exiting from relationships where sensitive code owned by the FI is hosted outside the FI's infrastructure, FIs must ensure it is irrecoverably deleted from the third party's environment.

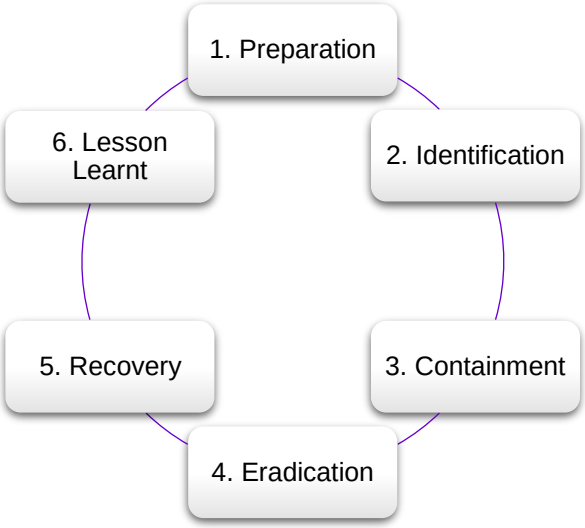
Third Parties

- Users must be authenticated prior to accessing sensitive source code repositories. Direct remote access to the repositories from untrusted / unmanaged environments should require additional controls.
- Access to sensitive source code repositories and artefacts must be granted on a least privileged basis and on strict need-to-have and need-to-know principles.
- Third parties should enforce strong password controls over users' access to source code repositories.
- All access to the sensitive source code repository should be logged. The audit log should be regularly reviewed for unauthorised access and other anomalies.
- There should be a process for reviewing requests for provisioning of accounts to sensitive code repositories. Entitlements to the sensitive source code repository must be regularly reviewed and revoked immediately upon change in user status, e.g. change in role, employment status etc.
- Existing data loss prevention solutions should contain rules specific to blocking sensitive source code from being sent externally.
- Strong end point controls should be implemented on the developer's endpoint devices that are used for accessing sensitive source code. Sensitive source code should not be accessed from unprotected endpoints.

4. INCIDENT RESPONSE AND MANAGEMENT PLAN FOR SOURCE CODE LEAKAGE

By establishing or augmenting existing incident response and management plan[3] to cover potential of source code leaks incidents, including leaks for codes owned and maintained by third parties, financial institutions can set out a consistent and effective approach to manage and response to the incidents. The key phases of a FI's incident response and management plan consist of *preparation*, *identification*, *containment*, *eradication*, *recovery*, and *lessons learned*.

[3] Refer to the MAS Technology Risk Management Guidelines Section 7.7 on Incident Management.



FIs could adopt similar plan to handle incidents related to source code leak by third parties. While considering the phases in the plan, it is important to note that the phases and responses will vary in different scenarios. For example, the response required in the case of source code leakage for the FI's critical internet facing transactional system would be very different from the response required in the case of source code leakage in a COTS tool used within the FI's internal networks.

4.1 Preparation

Preparation is the key to any effective response and management plan and FI should ensure that the parties involved have the necessary knowledge and training, resources and support to response effectively. The following should be considered in this phase:

- The plan should be documented, and the roles and responsibilities are defined and explained to the teams involved.
- The teams involved should be trained and have the necessary tools and support.
- FIs should ensure their system and software asset inventories and records are up to date, in order for the FI to quickly identify the systems that could be affected by the source code leakage.
- The risks associated with software and systems are recorded and kept up to date as FI will need to assess if the known risk items will be exacerbated by the code leakage.

4.2 Identification

As part of the contractual obligations discussed earlier in Section 3.2, FIs need to agree on the time window and method which third parties would notify them in the event of a source code leak; and third parties need to implement reporting mechanisms to ensure that FIs are notified in a timely manner as per the contractual agreements.

The FIs' threat intelligence monitoring processes should cover third parties providing critical software and monitoring for any breaches, including source code leaks.

FIs should ensure that third parties have mechanisms in place to detect identify threats, e.g. monitoring attempts to access sensitive code and looking for potential indications of exfiltration of sensitive source code via user endpoints and well as from servers.

4.3 Containment

Upon notification from the third party software vendor of a source code leakage incident, FIs should work with the third party to confirm the extent of the leakage and ensure that the task of containing the leak and preventing further leak is handled by them.

One of the key concerns of such leaks is that attackers are able to analyse the codes and identify vulnerabilities to compromise the application and data.

FIs should work with the third party software vendor to perform an impact analysis on the leaked codes on the target applications and environment and carrying out in-depth security code review of sensitive codes that are leaked. This could help FI identify and mitigate gaps and vulnerabilities that can potentially be exploited.

Where FIs assessed that the code leak could potentially lead to increase in the risk of attacks on the FI's system, FI should consider the following response:

- Increase the frequency of the security log monitoring and surveillance of the impacted system;
- Conduct log review on past archive logs to the point of source code leak to identity attempts to attacks and compromise the system; and
- Where required, expedite any outstanding corrective actions to address known security issues.

As outlined above, cooperation with third parties is crucial to identify the root cause and potential impact to the FIs. In evaluating third parties, FIs should ensure that they have the experience and capability to support their operational arrangements. This includes providing assistance as requested and applying patches to counter the latest security vulnerabilities.

4.4 Eradication

FI should monitor the progress of the third party software vendor in mitigating any gaps and eliminating the root cause of the breach. Where required, FIs or affected third parties should implement additional safeguards to prevent recurrence of such incidents, e.g. removal of malware and implementing additional security controls on source code repositories.

4.5 Recovery

Once temporary mitigation measures are completed, FIs should test and verify that impacted software and/or systems are functioning normally and that the software integrity is not compromised. If the risk of software integrity cannot be adequately addressed, depending on the risk appetite of the FI, FIs may consider alternatives such as implementing mitigating controls or migrating to alternative systems and/or third party software vendor.

4.6 Lessons Learnt

After the investigation has been completed, FI should obtain the feedback from the parties involved and look at the areas of improvement, such as developing monitoring plans to prevent similar future incidents; updating security policies and procedures; and communicating lessons learnt to relevant teams. FIs may also consider using existing channels for information sharing with peer FIs to increase awareness of such incidents.

On an ongoing basis, FIs should continually review lessons learnt and information shared within the industry and consider integrating them into their incident response and management plan.

Based on the root cause analysis and lessons learnt, third parties should also recommend new controls or processes to prevent similar future accidents from happening. Third parties supporting critical

functions should also be involved in planning and testing the effectiveness of the FI's updated incident response and management plans in a timely manner.

5. APPENDIX

5.1 Notable Recent Source Code Leakage Incidents

- Nissan Source Code Leaked via Misconfigured Git Server:

https://www.darkreading.com/risk/nissan-source-code-leaked-via-misconfigured-git-server/d/d-id/1339845

- Source code from dozens of companies leaked online

https://www.bleepingcomputer.com/news/security/source-code-from-dozens-of-companies-leaked-online/

- FBI: Hackers stole source code from US government agencies and private companies

https://www.zdnet.com/article/fbi-hackers-stole-source-code-from-us-government-agencies-and-private-companies/

- SolarWinds hackers accessed Microsoft source code, the company says

https://www.cnbc.com/2021/01/01/solarwinds-hackers-accessed-microsoft-source-code-the-company-says.html

5.2 References

1. MAS Technology Risk Management Guidelines

   3.4.2 The FI should assess and manage its exposure to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party before entering into a contractual agreement or partnership.

   3.4.3 On an ongoing basis, the FI should ensure the third party employs a high standard of care and diligence in protecting data confidentiality and integrity as well as ensuring system resilience.

   3.5.2 A background check on personnel, who has access to the FI's data and IT systems, should be performed to minimise this risk.

   9.1.3 For proper accountability, the FI should ensure records of user access and user management activities are uniquely identified and logged for audit and investigation purposes.

   9.1.4 The FI should establish a password policy and a process to enforce strong password controls for users' access to IT systems.

   9.1.6 The FI should ensure appropriate parties such as information asset owners perform periodic user access review to verify the appropriateness of privileges that are granted to users.

   9.1.7 Users should only be granted access rights on a need-to-use basis.

   9.3.1 Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorised access to the FI's IT environment.

   11.1.2 The FI should implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices. The FI should ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standards.

   11.1.3 Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.

2. MAS Outsourcing Guidelines

   3.1 "outsourcing agreement" means a written agreement setting out the contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement

   5.2.1 While an institution may delegate day-to-day operational duties to the service provider, the responsibilities for maintaining effective oversight and governance of outsourcing arrangements, managing outsourcing risks, and implementing an adequate outsourcing risk management

framework, in accordance with these Guidelines, continue to rest with the institution, its board and senior management.

5.4.1 In considering, renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangements.

5.4.2 The due diligence should also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement.

5.5.1 Contractual terms and conditions governing relationships, obligations, responsibilities, rights and expectations of the contracting parties in the outsourcing arrangement should be carefully and properly defined in written agreements.
5.6.2 An institution should take the following steps to protect the confidentiality and security of customer information:
(a) State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices
(c) Ensure the service provider is able to protect the confidentiality of customer information
(d) Review and monitor the security practices and control processes of the service provider on a regular basis.

3. ABS Guidelines on Control Objectives and Procedures for Outsourced Service Providers

Section II (a) Logical Security: Logical access to programmes, data, and operating system software is restricted to authorised personnel on a need-to-have basis.

Section II (f) Network and Security Management: Systems and network controls are implemented based on clients' business needs.

Section II (h) System Vulnerability Assessments

4. ABS Control Objectives and Procedures for Outsourced Service Providers FAQ

18. Are the OSPs' sub-contractors also subjected to the ABS Guidelines?

Yes, the OSPs' sub-contractors are also subjected to the ABS Guidelines and the OSPAR requirements. OSPs must obtain prior approval from their FI clients before they sub-contract any part of the FI's outsourcing arrangement with the OSP.

21. Outsourcing covers a wide range of services. Do OSPs need to comply with all the controls stated in the ABS Guidelines?

The types of controls OSPs needs to comply with depending on the types of services performed. The Entity Controls and the Service Controls of the ABS Guidelines are applicable to all types of services performed. However, the General IT Controls are applicable to OSPs where the outsourced service involved the provision of IT capabilities / services by the OSP.

5. ABS' Cloud Computing Implementation Guide

Section 4 Part B, Design and Secure the Cloud, Virtualisation, Containerisation and DevOps: Considerations for Standard Workloads and Considerations for Material Workloads

Section 4 Part B, Source Code Reviews: Considerations for Standard Workloads and Considerations for Material Workloads

5.3 Acknowledgements

The ABS Working Group Members:

1. Citibank (Working Group Lead)
2. BNP Paribas
3. Deutsche Bank
4. MAS
5. Standard Chartered Bank