SEC-203: Assessment Activity 1
Concept to real-world security incident

Name: Thanawin Pattanaphol **ID: 01324096**

This report documents the XZ security exploit that occurred in March 29, 2024.

Summary: The xz exploit was initiated by an online actor named “Jia Tan”, who orchestrated a sophisticated supply chain compromise, where, the actor would put pressure on the original head XZ Utils, into giving them the position of a co-maintainer of the project. After gaining the position as a co-maintainer, Jia Tan then uses that position to publish XZ version 5.6.0, the first XZ version to have the backdoor exploit, along with version 5.6.1, a more sophisticated version that hides any display of abnormal runtime behavior. The exploit works as through injecting a backdoor into the liblzma library and enable remote code execution via SSH. The victims of the exploit were the open-source community, specifically systems that rely on the xz-utils library. However, thanks to the swift discovery of a Microsoft employee, the malicious code was caught and then patched before being deployed in stable releases of major Linux distributions. Nonetheless, the potential damages of this exploit was huge, as several companies and users rely on the xz-utils library to perform their daily processes, the impact of this small exploit could lead to data breaches, and huge disruptions in IT services.

Questions:

1. Which characteristics are compromised: confidentiality, integrity and availability? Of which assets?

   This exploit had the potential to affect all three characteristics, as the exploit could have enabled remote code executions, which can then lead to enabling attacks to be able to access sensitive data stored on compromised systems (personal information, financial data, and others), thus, compromising confidentiality. The exploit compromised the integrity of the xz-utils library through the modification of the source code, as well as, compromising the availability of systems using the xz-utils libraries for their services.

2. What vulnerabilities were exploited?

   The xz-utils exploit did not exploit software vulnerabilities in a traditional sense, but, it had exploited other aspects, such as, the trust in open-source contributors, complex build processes; as it is more difficult to detect changes during code reviews, and the limitations of human code reviewers.

3. What could be done to prevent or stop the attacks? What could mitigate the damage?

   There are several measures that could have helped or stopped a similar-style attacks, through, a more detailed examination of “scrutiny” of less-known contributors via background checks, stricter code review processes, or increassd community oversight for critical components; a more improved code review process; better supply chain security measures, including verification of software integrity, sandboxing and isolation; strengthening build system security, detection mechanisms, and more community collaboration and information sharing.

References:

SEC-203: Assessment Activity 1
Concept to real-world security incident

Name: Thanawin Pattanaphol **ID: 01324096**

- https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/
- https://www.wired.com/story/jia-tan-xz-backdoor/
- https://tukaani.org/xz-backdoor/
- https://access.redhat.com/security/cve/CVE-2024-3094
- https://www.openwall.com/lists/oss-security/2024/03/29/4