TechXplore

Major security flaws in Java applications, European researchers warn

December 27 2023

Alexandre Bartel, Professor at Umeå University, has, in collaboration with European research colleagues, studied major weaknesses in one of the world's largest programming languages. Credit: Mattias Pettersson

Alexandre Bartel, Professor of Software Engineering and Security at Umeå University, in collaboration with several European researchers, has extensively analyzed weaknesses in software written in one of the world's most widely used programming languages.

"This involves flaws in the processes that retrieve and recreate information—such as customer accounts, transactions, or patient records. These vulnerabilities can create huge costs for businesses, governments and public authorities."

Java is behind applications used in mobile games, robots, embedded systems or business applications. Over the years, several security flaws have been reported and now European researchers have investigated whether and how these have been addressed.

They have looked at Java products that use deserialisation, the process of restoring packaged information to its previous state, such as user settings, game functions, shopping carts or banking applications, and carried out an in-depth analysis of existing vulnerabilities and attacks.

Big companies affected

"We have identified weaknesses and how they have been addressed. The problem is that the programmers seem to repeat the same mistakes over and over again and therefore reintroduce the vulnerabilities," Professor Bartel says.

In the study "An In-Depth Study of Java Deserialization Remote-Code Execution Exploits and Vulnerabilities," which was conducted in collaboration with Eric Bodden, Professor at Paderborn University, Yves Le Traon, Professor at the Université du Luxembourg and Imen Sayar, now researcher at INRIA, several examples are given:

- Flaws in PayPal's critical applications—gave access to production databases
- Vulnerabilities at the San Francisco Department of Transportation—the attackers gained control of 2,000 computers and blocked the payment systems

- Equifax, the largest US credit reporting agency in the US—suffered an attack in which the attacker managed to steal 147.7 million pieces of personal data

What the European researchers are seeing is that the flow of bytes, the flow of information, opens for modification by attackers. "It is during the actual deserialization process, when the information is recreated, that the attacker can gain total control over the receiving system. Even very small changes in the code can make systems vulnerable to attacks," Alexandre Bartel says.

Serious flaws

Most Java programs rely on external libraries and there is no easy way to fix the affected systems. Alexandre Bartel argues that to prevent security flaws from being introduced in new code, the developers should avoid using Java deserialisation altogether.

"Our findings suggest that the entire supply chain of the developed application should be thoroughly verified throughout the application's lifecycle. The findings are very serious as they have the potential to be costly, not only for companies but also for society at large," says Alexandre Bartel.

The study has attracted considerable interest and was published in the highly regarded and selective Transactions on Software Engineering and Methodology journal, TOSEM, of the Association of Computing Machinery, ACM. The findings were also presented at ICSE, the International Conference on Software Engineering, which is one of the most prestigious conferences in the field.

Bartel and his research group are now developing methods to more efficiently detect these vulnerabilities and prevent attacks.

Serialization and deserialisation

Processes in computer science that involve saving a data structure or object state in a format that can then be stored or transferred to another computing environment. It involves "translating" data structures into a stream of bytes to facilitate storage in, for example, a memory, a file or during data transfer to another machine.

Examples include: Pharmaceutical systems, where governments require packaging to be coded so that it can be tracked throughout the supply chain. Game development: to store and load game data such as player progress, settings and saved games. Financial sector: storage and transmission of data on financial transactions between banks and other financial systems.

Provided by Umea University

Citation: Major security flaws in Java applications, European researchers warn (2023, December 27) retrieved 8 May 2024 from https://techxplore.com/news/2023-12-major-flaws-java-applications-european.html