waves
ENTERPRISE

Assessing blockchain platform to secure enterprise data and infrastructure

2020

kaspersky BRING ON THE FUTURE

Kaspersky Enterprise Blockchain Security

Waves Enterprise brings an enterprise blockchain platform to the market capable of powering large-scale enterprise, national and public sector projects while simultaneously ensuring ultimate security and privacy for millions of records.

wavesenterprise.com

IT

- Headquartered in Moscow, Russia
- Founded in 2018
- Passed **Kaspersky Blockchain Application Security Assessment**

Waves Enterprise, a hybrid blockchain platform, combines permissioned public and private networks and introduces a modular encryption capability. The platform is ready for certification by local governments or regulatory bodies. When integrated with existing IT infrastructure, the Waves Enterprise solution unlocks the power of blockchain for corporate customers as well as for public services, digital government services and smart cities.

Securely processing and storing confidential information about individuals, assets and activities is an important function of any large organization. Blockchain solutions can transform and simplify these functions and take the efficiency of the administrative processes to the highest level. This will reduce bureaucracy, improve transparency and increase trust levels in data processing operations – providing a clear value for users.

Artem Kalikhov, CPO at Waves Enterprise explains: "When dealing with millions of records, security is the main priority. Both public sector and corporate data must be protected against unauthorized access and manipulation; failure is never an option.

"We offer our customers a combination of blockchain technology and customizable cryptography functionality, where blockchain is responsible for records immutability and the encryption module provides the necessary protection for sensitive and confidential information. Our solution is packed, documented and ready for certification by potential customers' local governments - to avoid any timing issues."

Maintaining trust levels

When it comes to enterprise-grade and public sector solutions, security breaches can adversely affect large amounts of confidential data and digital assets.

Blockchain technology has certain strengths and by design provides immutability to recorded steps and operations. However, blockchain could still be vulnerable to flaws and errors in the application code and its environment.

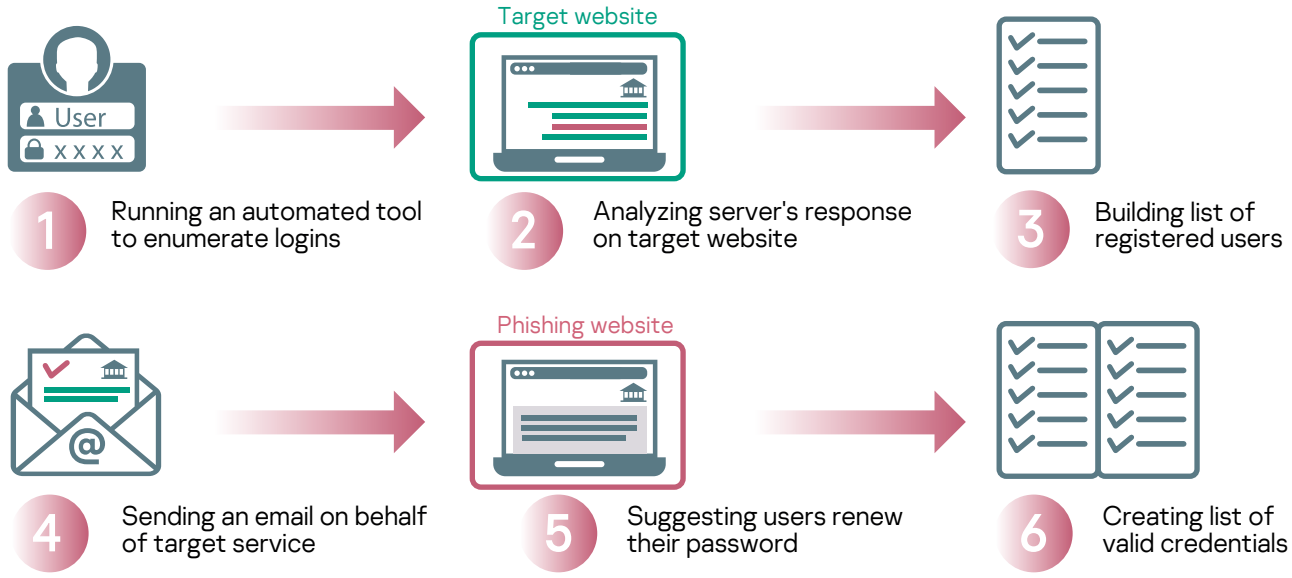
"Waves Enterprise Platform and the decentralized applications on top of it are intended to store and transfer confidential data. Given the risks associated with the application part of the solution, in order to deliver the value we promised we included checking and increasing the security level of the application side of the platform into our development lifecycle.

"To ensure a stable Waves Enterprise release, we teamed up with Kaspersky, a cybersecurity expert, for thorough testing of our solution components, including node implementation, the authorization service, and client-side code. We were aware of Kaspersky's expertise in various security segments and in DLTs in particular. Kaspersky has a proven track record in auditing blockchain platforms," – said Artem Kalikhov.

"To ensure a stable Waves Enterprise release, we teamed up with Kaspersky, a cybersecurity expert, for thorough testing of our solution components, including node implementation, the authorization service, and client-side code. We were aware of Kaspersky's expertise in various security segments and in DLTs in particular. Kaspersky has a proven track record in auditing blockchain platforms."

Artem Kalikhov, Chief Product Officer at Waves Enterprise

How enumeration attacks work



"Enumeration is a useful technique for revealing web-application vulnerabilities. One of the most common areas where it can be exploited is on a site's login, registration form or password reset page. Malicious actors are looking for differences in the server's response based on the validity of submitted credentials. When analyzing different scenarios, they are able to identify if the email is registered in the system and use this to create a list of valid users. The scammers can use this list for phishing attacks where emails supposedly sent from the compromised service contain requests for information or suggest actions disclosing valid credentials."

Pavel Pokrovsky, Blockchain Security Group Manager at Kaspersky

VERIFICATION
Code assessment by Kaspersky – an integral step prior to releasing Waves Enterprise Platform version 1.2 in March 2020.

DEMO
Kaspersky demo session showcased various scenarios using found vulnerabilities and illustrating their impact on Wave Enterprise solutions.

CONTRIBUTION
Kaspersky provided payloads and attack scripts for Wave Enterprise to integrate into automated test tools during the remediation phase.

White, grey or black: a solution that fits

"We started **Application Security Assessment** by deploying and configuring a test bed. In our case Kaspersky proposed using both black and grey-box methodologies: penetration testing first as an external attacker and then a legitimate user," – continued Artem Kalikhov.

"Depending on the client's needs we offer an appropriate solution. **Application Security Assessment** has 3 main options: **White-box**, which entails source code audit, **Grey-box** which entails emulating an attack posing as a legitimate user and **Black-box**, when we test resistance as an external attacker. Different options imply different time and resource consumption as well as a different price," – commented Pavel Pokrovsky, Blockchain Security Group Manager at Kaspersky.

"We appreciate that Kaspersky sharpened the assessment scope and proposed a service package that provided the best the budget vs value balance. This created a very professional atmosphere," – summed up the CPO of Waves Enterprise.

Assessment result

Artem Kalikhov described some aspects of the audit: "The assessment uncovered several vulnerabilities that would have impacted platform reliability, as well as the security of the applications built on top. Kaspersky experts ran a demo session for us showcasing each vulnerability and its impact on the system. Critical vulnerabilities were found in the platform environment, in the operating systems used in Docker images and in third-party libraries. Left unresolved, they would have resulted in denial of service, as well as unauthorized data disclosures."

"Enumeration is a useful technique for revealing web-application vulnerabilities. One of the most common areas where it can be exploited is on a site's login, registration form or password reset page. Malicious actors are looking for differences in the server's response based on the validity of submitted credentials. When analyzing different scenarios, they are able to identify if the email is registered in the system and use this to create a list of valid users. The scammers can use this list for phishing attacks where emails supposedly sent from the compromised service contain requests for information or suggest actions disclosing valid credentials," – explains Pavel Pokrovsky. – "While inspecting the "Forgot Password" functionality we discovered a username enumeration, which would allow attackers to detect valid Waves Enterprise usernames from a web application."

"In a nutshell, the remediation of this problem requires sending generic non-detailed server responses. On the other hand, UI designers work hard to provide the easiest and most intuitive interface to the user, and they sometimes choose usability over security basics. And yet there always needs to be a balance between user experience and security, and security should prevail for authorization services. This is why we involved independent security experts for auditing **how our application would resist hackers and malicious users**, making sure we keep the right balance in every single line of code," – continued Artem Kalikhov.

Secure Development Lifecycle: expert contribution

"Vulnerabilities can appear at every stage of development process. We at Waves Enterprise implemented Secure Development Lifecycle to deliver on customers' reliability expectations. Cooperation with Kaspersky, a leading cybersecurity expert, is part of our strategy to provide secure blockchain solutions to the corporate and public sectors.

"An important outcome of working with Kaspersky is their contribution to our secure development lifecycle. They shared a list of tools including payloads as well as test attack scripts, which we were able to build into our own automated test tools.

"We valued flexibility and the high level of support Kaspersky experts provided. Under the Kaspersky team's guidance, we quickly fixed all found vulnerabilities. The second **assessment confirmed the appropriate security level of our platform**, so we are now sure that we do not generate security risks for our customers. Kaspersky's assessment and guidance provide additional assurance of the security of the Waves Enterprise platform, bolstering confidence in the network," – summarized Artem Kalikhov.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com