



Risk level

0%

⌚ Low

Security report

LMoon

2 July, 17:18 — 3 July, 6:59

The date and time is in UTC

Summary

2 July, 17:18 — 3 July, 6:59

Risk level

0%

Low

There were 12 attacks detected from one IP address.

Attacks

12

ATTACKS
DETECTED
FROM 1 IP

Customers	4
Servers	6
Databases	2

Vulnerabilities

0

ACTIVE
VULNERABILITIES
TO MOMENT

Critical	0
Medium	0
Low	0

Incidents

0

SECURITY
INCIDENTS
FROM 0 IP

Customers	0
Servers	0
Databases	0

Recommendations

1. Immediately fix the vulnerabilities. Start with the critical ones.
2. Route the traffic for the web application through Wallarm nodes to detect and block malicious requests.



Vulnerabilities

2 July, 17:18 — 3 July, 6:59

A vulnerability is a defect or a weakness in the application – which can be a design flaw or an implementation bug – that allows an attacker to cause damage to the stakeholders of the application. Stakeholders include the application owner, application users, and other entities that rely on the application.

This report contains the information on the active and closed vulnerabilities discovered for the protected application(s).

The vulnerability descriptions are developer-friendly, task-based, and contain exact instructions on how to close them. Feel free to share this report with your engineers.

Dynamics

	AT BEGINNING OF THE PERIOD	DURING THE PERIOD FIXED / FOUND		AT THE END OF THE PERIOD
C Critical	0	0	0	0
M Medium	0	0	0	0
L Low	0	0	0	0
Sum total	0	0	0	0

- C Critical vulnerabilities are real threats to your data, servers, and customers. Fix them as soon as possible!
- M Medium risk vulnerabilities could be dangerous in some cases. Attackers often use them to evolve an attack.
- L Low risk vulnerabilities are not immediately dangerous. Attackers can use them as an aid in specific cases.

Attacks

2 July, 17:18 — 3 July, 6:59

An attack is a malicious activity by an attacker to find and exploit the vulnerabilities in applications. An attack consists of a number of requests – usually hundreds or thousands. If an application is protected with Wallarm, you can block these potentially malicious requests.




This report contains brief information about the attacks, but you can get detailed data on each malicious request detected using the Wallarm interface at <https://my.wallarm.com>.

Attacks

12

ATTACKS
DETECTED
FROM 1 IP

 Customers	4
 Servers	6
 Databases	2

-  Attacks on customers — XSS and other types of attacks which affect customers of application.
-  Attacks on the server side — RCE, XXE, and other types of attacks resulting in a remote code execution on the server side.
-  Attacks on databases — different types of injections in SQL and NoSQL databases. Mostly SQL injections.



Cross site Scripting (XSS)

4 attacks with 4 requests from 1 IP


Target: client



	THREAT	REQUESTS	DATE	IP	DOMAIN, PATH	STATUS CODE	PARAMETER	VECTOR EXAMPLE
1	0%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_a_value	ipt>alert("XSS");</script>
2	0%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_a_XML_XML_TAG_script_value	alert("XSS");
3	0%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_f88e15df6d_value	ipt>alert('union sel ... s')</script>
4	0%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_f88e15df6d_XML_XML_TAG_script_value	alert('union sel



SQL Injection (SQLi)

2 attacks with 2 requests from 1 IP

 Target: database

	THREAT	REQUESTS	DATE	IP	DOMAIN, PATH	STATUS CODE	PARAMETER	VECTOR EXAMPLE
1	 67%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_b_value	UNION SELECT ALL FROM information_sch ... AND ' or SLEEP(5) or
2	 67%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_f88e15df6d_XML_XML_TAG_script_value	ert('union select pas ... ers')



Remote Code Execution (RCE)

1 attack with 1 request from 1 IP

Target: server

THREAT	REQUESTS	DATE	IP	DOMAIN, PATH	STATUS CODE	PARAMETER	VECTOR EXAMPLE
1 100%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_d_value	bin/cat /etc/pas



Path Traversal

5 attacks with 5 requests from 1 IP



Target: server

	THREAT	REQUESTS	DATE	IP	DOMAIN, PATH	STATUS CODE	PARAMETER	VECTOR EXAMPLE
1	90%	1	2 July 2025, 22:45 2 July 2025, 22:45	50.39.179.7	35.224.102.117/etc/passwd	404	URI_value	/etc/passwd
2	90%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	URI_value	%2F%2F%2Fetc%2Fshadow%22%
3	90%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_e_value	EM "file:///etc/sha
4	90%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_d_value	at /etc/passwd; pi
5	90%	1	2 July 2025, 22:54 2 July 2025, 22:54	50.39.179.7	35.224.102.117/	200	GET_c_value	../etc/passwd

Security incidents

2 July, 17:18 — 3 July, 6:59

If Wallarm detects attacks targeting the application vulnerabilities, the system marks them as security incidents. Potentially each of these attacks could lead to a data breach!




The presence of security incidents is a situation that requires a mandatory response! It is recommended to limit the requests to the vulnerable part of the application with a virtual patch through Wallarm. Communicate the information about the vulnerabilities to the R&D and DevOps teams to start the incident investigation.

Incidents

0

INCIDENTS DETECTED
FROM 0 IP

	Customers	0
	Servers	0
	Databases	0

-  Some of the user accounts may have been compromised, or there were actions committed on behalf of the users.
-  On the web application servers, there were likely executed unauthorized commands, or the project files have been accessed.
-  Intruders potentially gained access to the information from the database that the application uses.