

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
			and gain unauthorized access to sensitive information.			
8614632	Low	Security Misconfiguration and Public Exposure - RDP Service is Observed on the Default Port (LOW)	Based on our observation, we noted that the RDP service is exposed to the public, it allows attacker to attempt to gain access to your network and sensitive information. Attackers can exploit vulnerabilities in RDP or employ brute force attacks to guess login credentials, leading to unauthorized access, data breaches, and manipulation of your systems. If the RDP service is open to the internet it becomes an entry point for an adversary to perform attacks.	Web Application	<ol style="list-style-type: none"> 13.13.61.42:3389/tcp 13.13.61.30:3389/tcp 13.13.61.97:3389/tcp 	<p>-For paid subscribers only-</p> <p>If you wish to subscribe, please contact our team</p>
8614613	Low	User Credentials Leak - Session Cookie Leaked Through Compromised Client (LOW)	<p>Based on our observation, we noted that your consumer accounts were compromised when logging in from a compromised client device. When using consumer accounts on a compromised client device, attackers can steal login credentials and gain unauthorized access to sensitive data. Compromised client devices are those that have been infected with malware or are otherwise under the control of an attacker. Attackers can use these devices to intercept login credentials, hijack user sessions, or perform other malicious activities.</p> <p>Stolen session cookies records: 40</p> <p><i>(Subscribe to uncover the compromised credentials)</i></p>	Web Application	1. sample.com	<p>-For paid subscribers only-</p> <p>If you wish to subscribe, please contact our team</p>
8614630	Low	Security Misconfiguration and Public Exposure - MySQL Service	MySQL is an open source Relational Database Management System (RDBMS)	Database	<ol style="list-style-type: none"> 13.13.61.15:3306/tcp 13.13.60.27:3306/tcp 	-For paid subscribers only-

Ticket Number	Exposure Risk	Title	Description	Attack Surface	Affected Target / Asset	Recommendations
		is Observed on the Default Port (LOW)	that utilizes Structured Query Language (SQL). Port 3306 is the default port used by MySQL protocol. It's used to connect to MySQL clients and utilities such as <i>mysqldump</i> . By having port 3306 unmonitored and opened to public access, data (except for passwords) are transmitted in clear, unencrypted form, and the protocol itself may be hacked to permit attackers access to your system.		3. 13.13.60.12:3306/tcp	If you wish to subscribe, please contact our team

---END OF REPORT---