### **SOC175 — PowerShell Found in Requested URL — Possible CVE-2022–41082 Exploitation**

#### **Alert: SOC175 — PowerShell Found in Requested URL — Possible CVE-2022–41082 Exploitation**

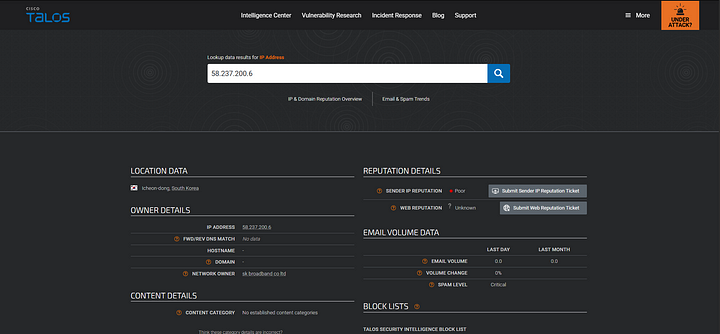
First, let us understand what exactly is CVE-2022–41082. It is a RCE(Remote Code Execution) vulnerability. In this vulnerability when auto discovery/autodiscovery.json is passed to the email field in the URL the Exchange server does not perform its checks and thorough normalization, leading to arbitrary access as NT AUTHORITY/SYSTEM. It is important to note that this vulnerability is often exploited in conjunction with CVE-2022–41040, a Server-Side Request Forgery (SSRF) vulnerability. CVE-2022–41040 allows an attacker to send requests to arbitrary URLs from the Exchange server. The SSRF vulnerability is exploited by manipulating the /autodiscover/autodiscover.json endpoint in the URL, allowing the attacker to potentially force the Exchange server to make a request to an unintended backend resource. Basically, if successful, this vulnerability provides access to a web shell. More can be read about this at [https://unit42.paloaltonetworks.com/](https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/) and [https://gteltsc.vn/](https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html)

Let us start the investigation.

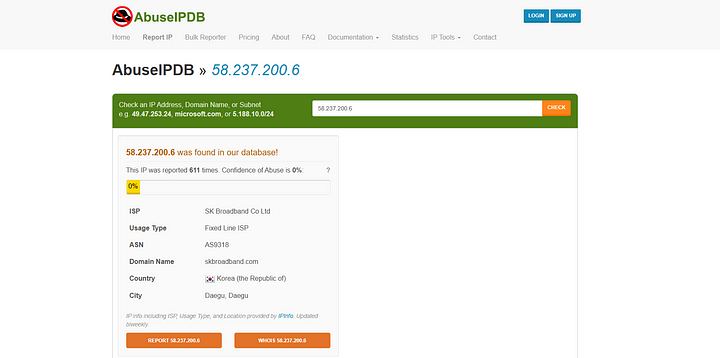
Let us first check the reputation of the IP address

Source IP : 58.237.200.6

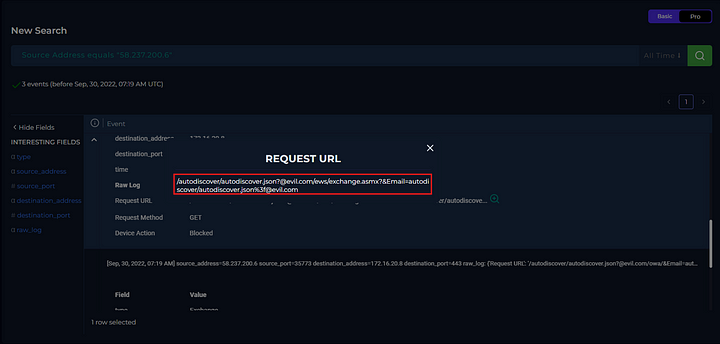
As per Cisco Talos, the location of the IP address is South Korea and the reputation is poor.



Same with AbusePBD. As per this the IP was reported 611 times and the confidence is 0%.



Now, let us check the logs.



We can see above that, the same URL which was mentioned on Unit42’s blog is present in the logs. But if we see the Device action all the three logs we can see that the URL’s were blocked and when checking the endpoint there were no signs of compromise. So we can conclude that this attack was unsuccessful.

Hence, we do not require to escalate this alert.

#### **Artefacts:**

**ALERT:** PowerShell Found in Requested URL — Possible CVE-2022–41082 Exploitation

**SRC\_IP:** 58[.]237[.]200[.]6

**DST\_IP:** 172[.]16[.]20[.]8

**URL:** /autodiscover/autodiscover.json?@evil.com/owa/&Email=autodiscover/autodiscover.json%3f@evil.com&Protocol=XYZ&FooProtocol=Powershell

**HOST:** Exchange Server 2

**ATTACK TYPE:** RCE(REMOTE CODE EXECUTION) and SSRF(SERVER SIDE REQUEST FORGERY)