**Postmortem of a system outage dated 02-02-2024**

**Summary**

On the date aforementioned at 1.00 a.m the system monitoring tool reported the homepage returning 404 (Page Not found) and 500 (Internal Server Error) errors. A couple of reports were also received from end users reporting slow load time and inaccessible pages.

The downtime was approximately 2hrs before it could be fully resolved affecting approximately 16% of online users.

**Timelines:**

* 02/02/2024: 0100hrs - The monitoring system started reporting downtime in the server and 404 errors from the logs.
* 02/02/2024: 0015hrs - A SOC analyst from the security department noticed the logs and forwarded a complaint to the engineering team for further scrutiny. Email reports from users were also received around the same time period.
* The engineering team started looking into the logs provided by the server and the first assumption of the root cause was a buffer overflow in one of the server’s memory.
* Further analysis showed that the load balancer wasn’t working as intended and all traffic was directed to only one server.
* An update to the load balancer software temporarily fixed the situation until the security team reported yet another issue with an attempted DDoS as the cause.
* The security team was able to block requests from the client IP address while the developers got to work to resolve a vulnerability that caused unauthorized access and possible memory breaching which was exploited by the attacker to cause a buffer overflow on the system.

**Root Cause**

There were two main causes to the system outage:

1. Disruption in the functionality of the load balancer

The software running on the load balancer was found to be out dated which led to traffic being directed to only one server.

This overloaded the server and caused lagging and downtime.

The attack was also able to gain advantage since they only had one server to attack this could have been disastrous whether known or unknown to the attacker.

1. Attempted DDoS Attack

The security team also noted an attempted DDoS on the server through an unpatched vulnerability on the webpage.

Thankfully the attack didn’t escalate much as it was not a high severity attack.

**Corrective and preventive measures**

Recommendations provided include:

* Occasional updates on the server and load balancers.
* Ensuring server memory space is always sufficient (more than 50% should always be available)
* Occasional security assessment of the system for vulnerabilities and necessary patching on any