|  |  |
| --- | --- |
| **Incident Report Information** **Incident Ticket Number:** #001\_270919 **Category:** Network **Sub-category:** Port **Priority:** Low **Status**: Close | **Contact Information for this Incident** **Name:** Kenny Kwek  **Title:**  IT Operations Manager & Support Manager  **Mobile Phone:**  9620 1737  **Email address:** kenny.kwek.2017@sis.smu.edu.sg |

# **Description of the incident:**

On 27 February 2019, at approximately 3.26 P.M, the team have detected that the port 8000, which the Smart Contract Product application is hosted on, was down. This was detected via Cloudtopus. Tier 3 was notified immediately and the issue was rectified at 3.52 P.M. After analyzing the incident, it was later found that the port was initially down on 27 February 2019, at approximately 8.30 A.M.

During the time of detection and rectification, the Smart Contract Product application was still running on a separately deployed port 8001.

# **Impact to business agreed service levels:**

Medium. Web application was still running due to load balancing, able to access via port 8001. No data was involved during this incident

(Refer to the “*Systems affected by Incident”* section for technical analysis of incident.)

|  |  |
| --- | --- |
| **Scope of Incident** | |
| **Number of sites affected by the incident:** | 0 |
| **Approximate number of systems affected by the incident:** | 0 |
| **Approximate number of users affected by the incident:** | 0 |
| **Are business partners affected by the incident?**  **(If Yes, please describe)** | No |
| ***Additional information:*** As the affected web server is for the sole purpose of displaying the web page on the latest launch updates of the Smart Contract Product, no user accounts or administrative accounts were affected. | |

# 

# **Additional Personnel notified of Incident**

Loc Hguyen Huynh Chief Operating Officer

Wendy Tan Product Manager

Ong De Lin Quality Assurance

Lee Jia Ern, Janell Tier 1 - Communication

Tan Rong Jian Mark Tier 2 - Business Analyst

Lau Jun Rong Tier 3 - Dev and Infrastructure & Security

|  |  |
| --- | --- |
| **Systems affected by Incident** | |
| **Attack Sources (e.g., IP Address, Port):** | Internal File, .trojan file |
| **Attack Destinations *(e.g., IP address, Port)*:** | Port 8000 |
| **IP Addresses of Affected Systems:** | <http://3.1.118.42:8000> |
| **Domain Name(s) of Affected Systems:** | [esmscp.tk:8000](http://www.esmscp.tk:8000) |
| **Primary Functions of Affected Systems:**  ***(e.g., Web Server, Domain Controller)*** | Web Server |
| **Operating Systems of Affected Systems:**  ***(e.g., Version, Service Pack, Configuration)*** | Amazon Linux, Linux Kernel 4.14. |
| **Patch Level of Affected Systems:**  ***(e.g., Latest Patches Loaded, Hotfixes)*** | Latest Patches Loaded |
| **Security Software Loaded on Affected Systems:**  ***(e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)*** | NIL |
| **Physical Location of Affected Systems:**  ***(e.g., State, City, Building, Room, Desk)*** | AWS Cloud |

|  |  |
| --- | --- |
| **Users Affected by Incident** | |
| **Names and Job Titles of Affected Users:** | N.A. |
| **System Access Levels or Rights of Affected Users: (e.g., regular User, Domain Administrator, Root)** | N.A. |
| ***Additional information:***  N.A. | |

|  |  |
| --- | --- |
| **Timeline of Incident** | |
| **Date and Time When Agency First Detected, Discovered, or Was Notified About the Incident:** | 27 February 2019, 3.36 P.M. |
| **Date and Time When the Actual Incident Occurred:**  ***(Estimate If Exact Date and Time Unknown)*** | 27 February 2019, 8.30 A.M. |
| **Date and Time When The Incident Was Contained or When All Affected Systems or Functions Were Restored:**  ***(Use Latest Date and Time)*** | 27 February 2019, 3.52 P.M. |
| **Elapsed Time Between the Incident and Discovery:**  ***(e.g., Difference Between a. and b. Above)*** | 7 hours 6 minutes (426 minutes) |
| **Elapsed Time Between the Discovery and Restoration:**  ***(e.g., Difference Between a. and c. Above)*** | 16 minutes |
| **Resolution Time (Elapsed Time Between the Incident and Restoration:** | 7 hours 22 minutes (446 minutes) |
|  | |

# **Incident Management**

**Action(s) Taken to Identify Affected Resources**

1. Monitoring of server status on Cloudtopus platform

**Action(s) Taken to Remediate Incident**

1. Rehosted Port 8000

|  |  |  |
| --- | --- | --- |
| **Walkthrough of Incident Timeline** | | |
| **Tier 1 - Communications** | | |
| **Steps** | **Description** | **Comment** |
| 1 | Access Cloudtopus Monitor Page | Check status of Web Application |
| 2 | Inform Tier 2 of Offline Web Application Status | Update Tier 2 of Web App Status “Down” |
| **Tier 2 - Business Analyst** | | |
| **Steps** | **Description** | **Comment** |
| 3 | Access Cloudtopus Monitor Page | Check status of Web Application |
| 4 | Access ‘esmscp.tk’ | Ensure website is running and can be accessed if one port is down |
| 5 | Access ‘esmscp.tk:8000’ and ‘esmscp.tk:8001’ | Find out which port is down  (port 8000) |
| 6 | Inform IT Operations Manager and Tier 3 | Immediately update relevant stakeholders that port 8000 is down |
| **Tier 3 - Dev and Infrastructure & Security** | | |
| **Steps** | **Description** | **Comment** |
| 7 | Access ‘esmscp.tk:8000’ on browser | Check port 8000 to confirm if really unavailable |
| 8 | Access the directory of application’s startup file ‘cd /home/ec2-user/Django\_Application/virtual\_env/ICA-1/ICA/bin’ | Get to the directory to start the startup file |
| 9 | Enter ‘Chmod +x auto\_start.sh’ | Give execution permission for the script |
| 10 | Enter ‘nohup ./auto\_start.sh’ | Start the script to launch the application on port 8000 without killing it even after exiting from the server |

# **Post-Incident Follow up**

Actions Planned to Prevent Similar Incidents: 1) Explore and set up more Cloudwatch alarms.

2) Implemented Nagios for better monitoring.

**Additional Remediation Details:**

Frequent monitoring will be carried out to ensure the earliest detection of the health of the server/ports as soon as possible.