IT Incident Reporting Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. 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](mailto:kenny.kwek.2017@sis.smu.edu.sg) | | | |
| **2. Incident Description**. | | | | |
| On 27 February 2019, at approximately 3.36 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 3.56 P.M.  During the time of detection and rectification, the Smart Contract Product application was still running on a separately deployed port 8001. | | | | |
| **3. Impact / Potential Impact** | | | | |
| Nil. Webapp was still running due to load balancing, able to access via port 8001. | | | | |
| **4. Sensitivity of Data/Information Involved (Insert tick on all that apply)** | | | | |
| |  |  |  |  | | --- | --- | --- | --- | |  | Critical Information |  | Personally Identifiable Information (PII) | |  | Non-Critical Information |  | Intellectual/Copyrighted Information | | **✓** | Publicly Available Information |  | Critical Infrastructure/Key Resources | |  | Financial Information |  | Unknown/Other (Please Describe Below) | | | | | |
| **5. Who Else Has Been Notified?** | | | | |
| |  |  | | --- | --- | | **Name** | **Role** | | Rafael J. Barros | Chief Operating Officer / Release Manager | | 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 | | | | | |
| **6. Incident Details** | | | | |
| Scope of incident | | | | |
| |  |  | | --- | --- | |  | **Critical** *(e.g., Affects State-Wide Information Resources)* | |  | **High** *(e.g., Affects Agency Entire Network or Critical Business or Mission Systems)* | | **✓** | **Medium** *(e.g., Affects Agency Network Infrastructure, Servers, or Admin Accounts)* | |  | **Low** *(e.g., Affects Agency Workstations or User Accounts Only)* | |  | **Unknown/Other** *(Please Describe Below)* | | | | | |
| 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 non-Commonwealth systems, such a business partners, affected by the incident?  (Y or N – if Yes, please describe) | | No | | |
| Please provide any additional information that you feel is important but has not been provided elsewhere on this form. | | 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. | | |

|  |  |
| --- | --- |
| **6. Systems Affected by Incident** *(Provide as much detail as possible)* | |
| Attack Sources *(e.g., IP Address, Port)*: | Suspected DDoS on Port 8000 |
| 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: | [www.esmscp.tk:8000](http://www.esmscp.tk:8000), 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 |
| *Additional System Details:* | |

|  |  |
| --- | --- |
| **7. Users Affected by Incident** *(Provide as much detail as possible)* | |
| 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 User Details:*  NIL | |

|  |  |
| --- | --- |
| **8. Timeline of Incident** *(Provide as much detail as possible)* | |
| a. Date and Time When Agency First Detected, Discovered, or Was Notified About the Incident: | 27 February 2019, 3.36pm |
| b. Date and Time When the Actual Incident Occurred:  *(Estimate If Exact Date and Time Unknown)* | 27 February 2019, 3.23pm |
| c. 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, 3.56pm |
| Elapsed Time Between the Incident and Discovery:  *(e.g., Difference Between a. and b. Above)* | 13 minutes |
| Elapsed Time Between the Discovery and Restoration:  *(e.g., Difference Between a. and c. Above)* | 20 minutes |

|  |  |
| --- | --- |
| **9. Remediation of Incident** *(Provide as much detail as possible)* | |
| Actions Taken To Identify Affected Resources: | Monitoring of server status on Cloudtopus platform |
| Actions Taken to Remediate Incident: | Rehosted Port 8000 |
| Actions Planned to Prevent Similar Incidents: | NIL. Backup ports are already in place to take over in case of any failure of a single port. |
| *Additional Remediation Details:*  Frequent monitoring will be carried out to ensure the earliest detection of the health of the server/ports ASAP. Will implement better monitoring tools like Nagios or implement better alerting tools. | |