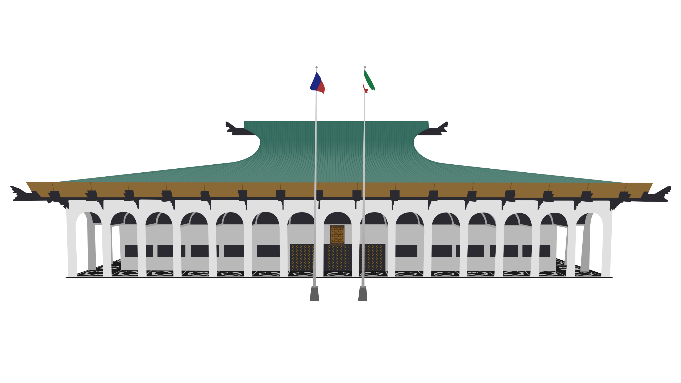
****

**BANGSAMORO GOVERNMENT**

**BANGSAMORO COMPUTER EMERGENCY RESPONSE TEAM**

**PHILIPPINES**

**(BCERT-PH)**

**BCERT.PH - INCIDENT NOTIFICATION REPORT**

|  |  |
| --- | --- |
| **NAME OF ORGANIZATION** | **BANGSAMORO DARUL-IFTA** |
| **TLP** | **AMBER+STRICT** |
| **Ticket No.** | **BCERT-PH #00001** |
| **NCERT Ticket No. (Optional)** |  |
| **Incident Name** | **Unauthorized File Upload and Website Defacement** |

*To know more of Traffic Light Protocol (TLP) visit https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.*

**LEAD RESPONDERS**

|  |  |
| --- | --- |
| ARNOLD S. CARARAG, Mbaex, MDM, MCS  Chief, Network and Security Management Section | DATU RAFFY RALPH S. SINSUAT, MSc.IT  Chief, Information Systems Development and Management Section |

**Confidentiality Statement:** This document contains confidential information exclusively for the eyes of the Head of Agency and is strictly prohibited from disclosure, distribution, or sharing with any unauthorized individuals or entities. Accessing this document implies an agreement to maintain its confidentiality and to utilize it solely for its intended purpose. Unauthorized reproduction, dissemination, or use of its contents may result in legal consequences. The recipient is responsible for safeguarding the document and preventing unauthorized access or disclosure. Thank you for your cooperation in upholding the confidentiality of this information.

**INCIDENT NOTIFICATION DETAILS**

|  |  |
| --- | --- |
| Incident Name | Unauthorized File Upload |
| Threat Level Indicator | **Elevated – Detected known vulnerabilities, Idle botnets and backdoors,**  **Unresolved signs of system intrusion (website defacements, etc.)** |
| Incident Origin / Channel | BICTO Threat Monitoring Team / TMT#2025-00001 |
| Date/Time Received | January 14. 2025, 1:50PM |
| Assigned Ticket Number | BCERT-PH #00001 |
| Assigned Responder | Arnold S. Cararag / Datu Raffy Ralph S. Sinsuat |
| Report Date | January 14, 2025, 1:52PM |
| Revision no./ Notes | Version 1.0 / For transmittal to and resolution of Bangsamoro  Autonomous Region in Muslim Mindanao – Bangsamoro Darul-Ifta |
| Incident Background | BCERT-PH, through OSINT, has monitored an Unauthorized File Upload on the website of Bangsamoro Autonomous Region in Muslim Mindanao – Bangsamoro darul-Ifta. Unauthorized file upload and defacement refers to the act of uploading files to a system or website without proper authorization or permission. Additionally, the unauthorized modification of the user interface of the website. |
| Evidence / Artifacts | |
|  | |
| Incident Findings/ Analysis | |
| With the available artifacts and information, BCERT-PH verified the said Unauthorized File Upload. | |
| Threat Vectors/ Incident Type/ Description | |
| Attack Vector: Attrition, Vulnerabilities  Incident Type and Description: Unauthorized File Upload and defacement- a type of security attack when an attacker gains access to a website/website server and upload unauthorized file and replace content on the site with their own messages. This is carried out to gain publicity or to spread a message. | |
| Impact Classification Rating | |
| Functional: While there is no effect yet on the current organizational functionality, there is an impact on the integrity, confidentiality, and availability where there is an unauthorized access and the possibility of data breaches of personal data collected/stored at the website/server.  Information – INTEGRITY – Integrity Loss; Sensitive or was changed or deleted.  Recoverability – REGULAR – Regular; Time to recovery is predictable with existing resources.  Note: impact classification may be elevated to a higher impact once incident is observed or verified | |
| Actions Taken and Recommendation | |
| It is crucial to pinpoint the point of entry or vulnerability that the threat actor used to carry out his unauthorized activities. BCERT-PH recommends the following.   * BICTO incident response team immediate sent a ticket to Darul-Ifta regarding the breach. * Gather security logs, evidence and artifacts of the affected system to understand how the attacker gains access. These logs can be sent to CERT-PH for further investigation. * After gathering BICTO shutdown the Darul-Ifta website to prevent escalation and reputation risk. * Remove the unauthorized file uploaded and check your web server if there are other malicious files   or code uploaded.   * Notify your hosting provider of the attack and ask them for assistance in securing your website. * Change the login credential and implement strong and complex password policy. * Implement monitoring system to review network activities regularly. Ensure that only authorized users have access to sensitive areas of the website * Utilize firewalls and network security measures to restrict outgoing connections from the server. * Ensure that the installed CMS, plug-ins, database, and other technologies used in your website are in   their latest versions.   * Provide security awareness training to website users and administrators. * Implement strict file upload restrictions and conduct a thorough security audit of web server and   application to identify any vulnerabilities or weaknesses.   * Implement a website backup and disaster recovery plan. * You may request for Vulnerability Assessment and Penetration Testing (VAPT) service of critical   systems identified by your organization from BCERT-PH.  Note: Please be informed that your internal security team can re-assess and re-confirm the detected threats/vulnerabilities to verify and tag the incidents as a false positive or true positive for further investigation | |
| BCERT-PH Contact Information | |
| For inquiries and further assistance do not hesitate to contact us at.  ARNOLD S. CARARAG, Mbaex, MDM, MCS  Chief, Network and Security Management Section  [nsms@bicto.bangsamoro.gov.ph](mailto:nsms@bicto.bangsamoro.gov.ph)  09177039488  DATU RAFFY RALPH S. SINSUAT, MSc.IT  Chief, Information Systems Development and Management Section  [isdms@bicto.bangsamoro.ph](mailto:isdms@bicto.bangsamoro.ph)  09985770654  Bangsamoro Information and Communications Technology Office  Landline: 064-5572624 | |