Incident Reporting Form

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| **I am:**  the effected entity ☑ reporting incident affecting other entity | | | | |
| **Contact Information of the Reporter** | | | | |
| Name & Role/Title |  Individual ☑ Organization | | | |
| Organization name (if any) | CatchPhish | | | |
| Contact No. | 8779959071 | | Email: | catchphish@gmail.com |
| Address: | Kj Somaiya college of engineering | | | |
| **Basic Incident Details** | | | | |
| Affected entity  (if not same as reporting entity above) | | Union bank of India | | |
| Incident Type | | | | |
| Targeted scanning/probing of critical  Data Breach Attacks or malicious/suspicious activities  networks/systems  Data Leak affecting systems/ servers/ networks/  Compromise of critical systems/information Attacks on Internet of Things (IoT) devices software/ applications related to Big Data,  Unauthorised access of IT systems/data and associated systems, networks Block chain, virtual assets, virtual asset  Defacement or intrusion into the website software, servers exchanges, custodian wallets, Robotics, 3D  Malicious code attacks Attacks or incident affecting Digital and 4D Printing, additive manufacturing,  Attack on servers such as Database, Mail and DNS Payment systems Drones  and network devices such as Routers Attacks through Malicious mobile Apps Attacks or malicious/ suspicious activities  ☑Identity Theft, spoofing and phishing attacks Fake mobile Apps affecting systems/ servers/software/   DoS/DDoS attacks  Unauthorised access to social media applications related to Artificial Intelligence  Attacks on Critical infrastructure, SCADA and accounts and Machine Learning operational technology systems and Wireless Attacks or malicious/ suspicious activities  Other (Please Specify)  networks affecting Cloud computing ----------------------------------------------------------  Attacks on Application such as E-Governance, E- systems/servers/software/applications  Commerce etc. ---------------------------------------------------------- | | | | |
| Is the affected system/network critical to the organization’s mission? (Yes / No). (Brief details.) | | Yes | | |
| Basic Information of Affected System (Provide information that is readily available.) | | Domain/URL: http://claude.ai IP Address: 160.79.104.10 Operating System:Unknown (Hosting Server Details Not Available) Make/ Model/Cloud details: Hosted by MarkMonitor, Inc. Affected Application details (If any): Potential phishing website at claude.ai Location of affected system (including City, Region & Country): CA, US  Network and name of ISP: MarkMonitor, Inc., IP: 160.79.104.10 | | |
| Brief description of Incident: A potential phishing website was detected at claude.ai. Risk Score: 33.78/10 (Confidence: Low). The site was created on 04/08/2018 21:18 UTC.   Risk Analysis: - The HTML lacks a login form, so it's neither legitimate nor illegitimate. There are no input fields for username or password to assess. Therefore, there is no means to conduct credential harvesting. - Brand impersonation is possible, but difficult to assess fully with only the HTML. The presence of the 'Claude' name and Anthropic's description in the meta tags suggests it's attempting to represent Claude, which is expected. To determine if it's a malicious impersonation, the context of where the HTML is hosted needs to be considered (e.g. is the URL claude.ai, or a suspicious lookalike?). However, the presence of links such as `https://claude.ai/images/claude\_ogimage.png` do increase the likelihood that this is a legitimate resource. - The presence of numerous JavaScript files loaded from `/\_next/static/chunks/` indicates a complex application likely built with Next.js. While the scripts have nonces (d42c8206-cbc5-4fc0-a560-6b0c3a97b7bb), suggesting an attempt to implement Content Security Policy (CSP), without analyzing the javascript, it's impossible to definitively rule out malicious behavior. The `googletagmanager.com` inclusion also warrants a small amount of caution. - Social engineering is possible, especially if the user is directed to a fake website or page that looks legitimate. The presented HTML would provide a loading page, followed by a javascript call. The purpose of this page might be to load malicious code.  The domain is registered with MarkMonitor, Inc.. VirusTotal scan shows 0 engines flagged this domain as malicious out of 94 total engines. Immediate intervention is recommended to prevent potential data theft and financial fraud. | | Occurrence date & time (dd/mm/yyyy hh:mm): 04/08/2018 21:18 UTC Detection date & time (dd/mm/yyyy hh:mm): 17/03/2025 21:06 UTC | | |
| **Note:** (i) This form provides general guidance in terms of information which could be relevant to the incident.   1. It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form. 2. Reporting entity may, if desired, also provide relevant information other than mentioned in this form. | | | | |
| **Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at:** [**incide**](mailto:incident@cert-in.org.in)[**nt@cert-in.org.in**](mailto:nt@cert-in.org.in) | | | | |