Form to report Incidents to CERT-In			
For official use only:		Incident Tracking Number : **CERTIn-xxxxxx**	
1. Contact Information for this Incident:			
Name:	Organization:	Title:	
Phone / Fax No:	Mobile:	Email:	
Address:			
2. Sector : (Please tick the appropriate choices)			
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other _____
3. Physical Location of Affected Computer/ Network and name of ISP.			
4. Date and Time Incident Occurred:			
Date:	Time:		
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details.			

6. Information of Affected System:				
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model

7. Type of Incident:		
Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service(DoS) Distributed Denial of Service(DDoS) User Account Compromise	Website Intrusion Social Engineering Technical Vulnerability IP Spoofing Other_____
8. Description of Incident:		

9. Unusual behavior/symptoms (Tick the symptoms)	
System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.

12. Agencies notified?			
Law Enforcement	Private Agency	Affected Product Vendor	Other_____

11. When and How was the incident detected:

13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)	
Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION

14. IP Address of Apparent or Suspected Source:	
Source IP address:	Other information available:

15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected		
1 to 10	10 to 100	More than 100
17. Actions taken to mitigate the intrusion/attack:		
No action taken System Binaries checked	Log Files examined System(s) disconnected form network	Restored with a good backup Other_____
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident		
Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in		