|  |  |
| --- | --- |
| CONTACT INFORMATION | |
| Team Number | Team 2 |
| Time Incident Identified | 11/16/2024 |
| Target of Attack | Win0 |

|  |  |
| --- | --- |
| BUSINESS IMPACT | |
| Attack Vector | Passive |
| Functional Impact | Added SSHD and an SSH server and attackers listening on Port 22 |
| Information Impact | Allows for connection, Information and Data Loss |
| Recoverability | Removal of Users and SSH |

|  |  |  |  |
| --- | --- | --- | --- |
| DESCRIPTION OF INCIDENT/ACTIVITY | | | |
| Time First Identified | 8:06:50am PT | Time Last Identified | 8:06:50am PT |
| System(s) Impacted | Added SSHD | User(s) Impacted | Added SSHD |
| Record(s) Impacted | Potential records or data loss | Location(s) of Observed Activity | Win0 |
| Executive Summary: We discovered on 11/16/2024 8:06:50am PT that a Malicous user was created, called Win0$. This user then installed an SSH Client and Server onto Win0. This opened Win0 which is a system logging and Data storage server. This presents opportunity for compromised Data of users and system. They also took down Fire walls and other necessary protections. | | | |
| Indicators of Compromise/ Root Cause of incident: The firewall Is turned off so the system lacks basic security which allow vulnerabilities within the system to be exploited (attackers listening on port 22) | | | |
| Mitigation Action Taken (if any):  Remove the User and the deleting the SSH  Request the staff to change their password  Create awareness among the staff on safe use of Internet | | | |
| Lessons Learned/Opportunity for Improvement  Creating more awareness about Phishing attacks  Ensuring that the system was properly set up.  Proper monitoring of the system network  Consistent digital forensics | | | |

|  |
| --- |
| Supporting Artifacts Page \_\_\_ of \_\_\_ |
|  |