

# Ticket Details

--> Ticket ID:- 310

--> Title:- kmlknlnkn

--> Raised At:- 2024-09-25 16:38:17

--> Description:- Computer security (also cybersecurity, digital security, or information technology (IT) security) is the protection of computer software, systems and networks from threats that may result in unauthorized information disclosure, theft of (or damage to) hardware, software, or data, as well as from the disruption or misdirection of the services they provide.[1][2] The field is significant due to the expanded reliance on computer systems, the Internet,[3] and wireless network standards. It is also significant due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant new challenges facing the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance.[4][5] While many aspects of computer security involve digital security such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering. IT security is not a perfect subset of information security, thus does not fit completely into the security convergence schema. Vulnerabilities and attacks Main article: Vulnerability (computing) A vulnerability refers to a flaw in the structure, execution, functioning, or internal oversight of a computer or system that compromises its security. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.[6] An exploitable vulnerability is one for which at least one working attack or exploit exists.[7] Actors maliciously seeking vulnerabilities are known as threats. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts.[8][9] Various people or parties are vulnerable to cyber attacks; however, different groups are likely to experience different types of attacks more than others.[10] In April 2023, the United Kingdom Department for Science, Innovation & Technology released a report on cyber attacks over the last 12 months.[11] They surveyed 2,263 UK businesses, 1,174 UK registered charities, and 554 education institutions. The research found that "32% of businesses and 24% of charities overall recall any breaches or attacks from the last 12 months." These figures were much higher for "medium businesses (59%), large businesses (69%), and high-income charities with £500,000 or more in annual income (56%)."[11] Yet, although medium or large businesses are more often the victims, since larger companies have generally improved their security over the last decade, small and midsize businesses (SMBs) have also become increasingly vulnerable as they often "do not have advanced tools to defend the business." [10] SMBs are most likely to be affected by malware, ransomware, phishing, man-in-the-middle attacks, and Denial-of Service (DoS) Attacks.[10] Normal internet users are most likely to be affected by untargeted cyberattacks.[12] These are where attackers indiscriminately target as many devices, services, or users as possible. They do this using techniques that take advantage of the openness of the Internet. These strategies mostly include phishing, ransomware, water holing and scanning.[12] To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the following categories: Backdoor A backdoor in a computer system, a cryptosystem, or an algorithm is any secret method of bypassing normal authentication or security controls. These weaknesses may exist for many reasons, including original design or poor configuration.[13] Due to the nature of backdoors, they are of greater concern to companies and databases as opposed to individuals. Backdoors may be added by an authorized party to allow some legitimate access or by an attacker for malicious reasons. Criminals often use malware to install backdoors, giving them remote administrative access to a system.[14] Once they have access,

cybercriminals can "modify files, steal personal information, install unwanted software, and even take control of the entire computer." [14] Backdoors can be very hard to detect and are usually discovered by someone who has access to the application source code or intimate knowledge of the operating system of the computer. Denial-of-service attack Denial-of-service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. [15] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of distributed denial-of-service (DDoS) attacks are possible, where the attack comes from a large number of points. In this case, defending against these attacks is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including distributed reflective denial-of-service (DRDoS), where innocent systems are fooled into sending traffic to the victim. [15] With such attacks, the amplification factor makes the attack easier for the attacker because they have to use little bandwidth themselves. To understand why attackers may carry out these attacks, see the 'attacker motivation' section.

--> Remark:- None  
--> Severity:- S1  
--> Priority:- P1  
--> Raised By Id:- 26  
--> Updated At:- None  
--> Bucket:- venkatasivan  
--> Status:- open  
--> File Paths:- []

## Resolutions

--> Resolution Description:- skldlaldnalsdls  
--> Supporting Files:- []

## Audit logs

--> Event Description: Ticket created with number:310 and assigned to group L1.  
--> Event DateTime: 2024-09-25 16:38:17  
--> Event Description: Ticket picked up by user revanthv.  
--> Event DateTime: 2024-09-25 16:38:26  
--> Event Description: User revanthv assigned ticket to group L2.  
--> Event DateTime: 2024-09-25 16:40:00  
--> Event Description: Ticket picked up by user vaibhavr.  
--> Event DateTime: 2024-09-25 16:40:14  
--> Event Description: User vaibhavr assigned ticket to group L3.  
--> Event DateTime: 2024-09-25 16:46:39  
--> Event Description: Ticket picked up by user purur.  
--> Event DateTime: 2024-09-25 16:49:44  
--> Event Description: Resolution submitted by purur  
--> Event DateTime: 2024-09-25 16:49:53  
--> Event Description: User purur assigned ticket to group CL1.  
--> Event DateTime: 2024-09-25 16:58:22  
--> Event Description: Ticket picked up by user rishabhl.  
--> Event DateTime: 2024-09-25 16:58:55  
--> Event Description: User rishabhl assigned ticket to user 30.

--> Event DateTime: 2024-09-25 17:00:06