1. Using the Internet, browse to<https://www.kb.cert.org/vuls/> and find the most recent CERT advisory. Summarize three of the most recent vulnerabilities posted on this site.

MySQL for Windows contains a privilege escalation vulnerability due to the use of an OPENSSLDIR variable that specifies a location where an unprivileged Windows user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. By the same token, pulse Connect Secure (PCS) gateway contains a vulnerability that can allow an unauthenticated remote attacker to execute arbitrary code. By making a crafted request to a vulnerable Pulse Connect Secure system, an unauthenticated remote attacker may be able to execute arbitrary code on the gateway. Pulse Secure recommends disabling the two affected feature sets on existing PCS instances: Windows File Share Browser, Pulse Secure Collaboration. That aside, Atlassian Bitbucket on Windows fails to properly set ACLs, which can allow an unprivileged Windows user to run arbitrary code with SYSTEM privileges; an unprivileged user may be able to execute arbitrary code with SYSTEM privileges on a Windows system with the vulnerable Bitbucket software installed. To resolve the issue, apply an update to the new Bitbucket software version.

1. Using the Internet, find and read the SANS/FBI Top 20 Vulnerabilities. Summarize one of the 20 vulnerabilities listed and identify the threat group and threat category it warns about.

Memory Buffer Error: This flaw is usually introduced during Architecture and Design, Implementation, Operation stages of the SDLC. This buffer overflow happens when an application process tries to store more data than it can hold in the memory. Since the buffers can only store some level of data and when that level is reached and exceeded, the data flows to another memory location which can corrupt the data already contained in that buffer. This incident sometimes happens accidentally through some programming error or orchestrated by cybercriminals, the aftereffect could be disastrous, as this can erase data, steal confidential information, and even the whole application could crash because of this buffer overflow.