Assignment 1

(Syrrmlla@memphis.edu/U00839259)

Vulnerability #1: CVE-2021-26855 (Microsoft Exchange Server)

Versions 2013, 2016, and 2019 of Microsoft Exchange Server contain the significant vulnerability CVE-2021-26855, which was discovered by Microsoft. The flaw makes it possible for a remote attacker to run arbitrary code on a server without needing to be authenticated.

The NVD gave the vulnerability a CVSS base score of 9.1 (CVSS version 3.x) and 10 (CVSS version 2.0) after it was first reported on March 2, 2021. On-premises Microsoft Exchange Servers are affected by the flaw, and its exploitation might jeopardize the entire system.

The server-side request forgery (SSRF) weakness in Exchange Server is what makes the vulnerability possible for an attacker to make a specially designed request to the server and execute remote code. On March 2, 2021, Microsoft announced emergency fixes and severely urged all Exchange Server users to apply them right away.

System administrators and security teams should examine their systems for indications of exploitation and take corrective action as needed, including analyzing logs and locating any unwanted access. Also, due to the fact that CUs contain crucial security and non-security upgrades for Exchange Server, Microsoft advises organizations utilizing Exchange Server to install the most recent Cumulative Update (CU) for their version of Exchange Server.

It is crucial to remember that while installing the patch will guard against the CVE-2021-26855 issue, it will not fix any possible harm that may have already been done to a system if the vulnerability was exploited prior to installing the patch. Thus, it is advised that businesses do an in-depth security audit of their Exchange Server systems to make sure there hasn't been any data loss or unauthorized access.

Reference Link: https://nvd.nist.gov/vuln/detail/CVE-2021-26855

Vulnerability #2: CVE-2021-21972 (VMware vCenter Server)

CVE-2021-21972 is a vulnerability that was discovered in VMware vCenter Server, a widely used data center management tool. The vulnerability was disclosed in February 2021 and was given a Common Vulnerabilities and Exposures (CVE) identifier.

An attacker might remotely execute code on the vulnerable vCenter Server without any authentication because the vulnerability is a remote code execution problem. This might result in the server being completely compromised, giving an attacker the ability to steal critical information, put malware in place, and seize control of the entire vCenter Server system.

Several businesses utilize vCenter Server versions 6.5, 6.7, and 7.0 for virtualization and cloud computing, which are impacted by the vulnerability. The vRealize Operations plugin, which is by default activated in vCenter Server, has a bug that is responsible for the vulnerability.

An attacker may be able to send a specially constructed request to the vCenter Server thanks to the vulnerability, which is brought about by a problem with improper authentication in the vRealize Operations plugin. The request can then be used to run any command on the vCenter Server with administrative rights. By sending a carefully crafted request to the vCenter Server, an attacker might take advantage of this vulnerability and execute malicious code without any authentication.

On February 23, 2021, VMware issued a security update to fix this vulnerability and advised all users to do the same. VMware further advised customers to deactivate the vRealize Operations plugin up until the patch could be applied.

It's crucial for users of VMware vCenter Server to make sure they are running the most recent version of the software and have applied the security update supplied by VMware because the CVE-2021-21972 vulnerability has a high severity level. Failing to do so could lead to a security breach, which could have serious repercussions for the business in question.

Reference Link: https://nvd.nist.gov/vuln/detail/CVE-2021-21972