CORVIT

(Ethical Hacking)

Submitted To: Sir Bilal

Submitted by: Laiba Rehman

.....

Detailed Report on CVE-2024-20899

Purpose:

This report provides an in-depth analysis of CVE-2024-20899, a significant security vulnerability that can lead to Remote Code Execution (RCE). Disclosed in 2024, this vulnerability affects certain versions of Microsoft Exchange Server and poses critical risks to affected systems.

CVE Identifier:
CVE-2024-20899

Published Date:
August 14, 2024

Vulnerability Name:
Microsoft Exchange Server Remote Code Execution Vulnerability

Affected Software/Systems:

- **Software:** Microsoft Exchange Server
- **Versions Affected:**
    - Microsoft Exchange Server 2019 (before CU14)
    - Microsoft Exchange Server 2016 (before CU22)

Impact:

- **Remote Code Execution:** Attackers can execute arbitrary code on the server, which could lead to complete control of the affected system.
- **Privilege Escalation:** Successful exploitation could allow attackers to elevate their privileges on the server or network.
- **Denial of Service (DoS):** Although the primary impact is RCE, exploitation might also destabilize or crash the Exchange Server.

Summary: CVE-2024-20899 is a severe remote code execution vulnerability in Microsoft Exchange Server affecting versions before CU14 for Exchange Server 2019 and before CU22 for Exchange Server 2016. It allows remote attackers to execute arbitrary code with the same privileges as the server, posing significant risks. Immediate application of the provided patches and following best security practices are crucial to mitigate the risks associated with this vulnerability.

THE END