***Graphical user interface, text

Description automatically generated***

One of the vulnerabilities detected after scanning Windows Server 2008 is MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) (EMERALDTHREAD). It is a vulnerability with critical severity. The Print Spooler service is a file that can be executed and is active as long as the operating system is turned on. This particular service oversees processes involving printing such as acquiring the printer driver’s location, loading it and print job scheduling. There is a service impersonation vulnerability existing in the Print Spooler service version installed in the victim machine. Arbitrary code can be executed by attackers on a Windows XP system to gain unauthorized access to other Windows systems that are supported. Successful exploitation would result in an attacker having full power over a system affected by the vulnerability. The attacker would then have the permission to download software; read, alter, or remove data; and even register new accounts.

The vulnerability exists because the victim machine contains a print spooler interface exposed over Remote Procedure Call (RPC). An attacker might take advantage of systems using printer sharing and access the printer share to send uniquely crafted print requests. Its existence is due to the insufficient user permission restriction from Windows Print Spooler allowing attackers to access print spoolers with ease.

An attacker can exploit this vulnerability by sending malicious print requests to a system that is vulnerable like the scanned victim machine. It also fulfils the criteria mentioned above where it has a print spooler interface exposed over RPC. Remote users are not properly validated by the system being attacked to determine whether they possess enough permissions. As a result, attackers are given permission to create a file in a system directory with Windows as its operating system.

An example where this vulnerability has been exploited in the real world is EMERALDTHREAD. It is the codename given to this zero–day exploit. Hence, it is written in parenthesis at the end of vulnerability’s name. The exploitation was disclosed on the 14th of April 2017 and leaked by a group that goes with the name of Shadow Brokers. It is a hacker group responsible for releasing Equation Group exploits that specifically target Windows platforms. Along with the release of exploits includes FuzzBunch which is a hacking framework used to exploit systems that run Windows.

To solve MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) (EMERALDTHREAD), a set of patches has been released by Microsoft for Windows Server 2008 along with the release of MS17-010. The way the Printer Spooler service verifies access to print spoolers is corrected in this update. Users who have automatic updating turned on will not have to install the update manually. As for those who have not, it is recommended that the patches are applied in the nearest future through update management software. Users can also go to Microsoft Update Catalog to download the security update for their operating system. However, unfortunately for outdated Windows operating systems, they remain vulnerable as software updates are not provided anymore.

A picture containing treemap chart

Description automatically generated

Step 1: Go to Microsoft Update Catalog and search for the security update for Windows Server 2008 by entering the vulnerability’s code in the search box. Click on “Search”.

Graphical user interface, application

Description automatically generated

Step 2: Select the correct security update for Windows Server 2008 and click on “Download”.

Graphical user interface, text, application, email

Description automatically generated

Step 3: Click the link in the dialog box.

Graphical user interface, text, application, email

Description automatically generated

Step 4: Open the Microsoft Update Standalone Package with Windows Update Standalone Installer and click “OK”.

Graphical user interface, text, application

Description automatically generated

Step 5: Click “OK” to download and install the security update.

Graphical user interface, text, application, email

Description automatically generated

Step 6: Wait for the installation to be completed. Once done, the computer has to be restarted so that the updates installed take effect. Click on “Restart Now”.