Microsoft released an updated patch for 25 critical security holes

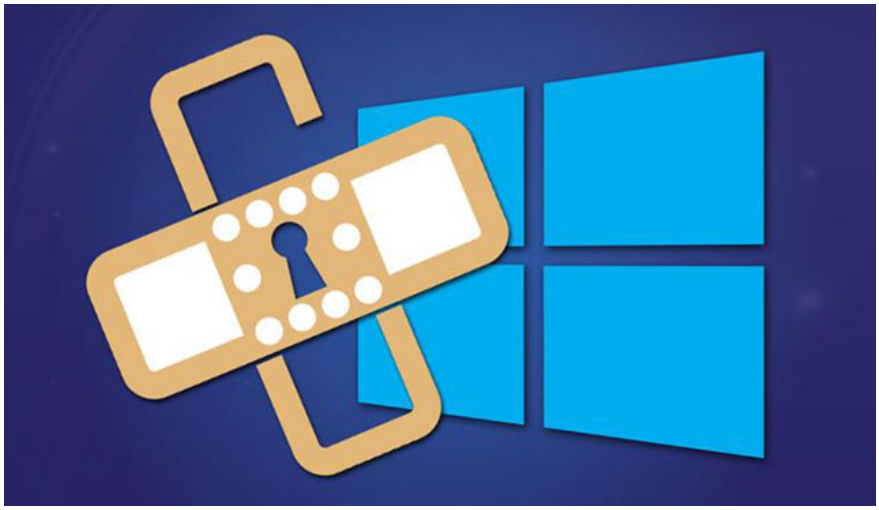
As part of August Patch Tuesday, Microsoft yesterday announced the release of 48 security updates for all supported Windows operating systems and other products.

The latest security update helps patch many vulnerabilities, including 25 very important errors, 21 critical errors and 2 average errors. These vulnerabilities affect many different versions of Windows OS, Internet Explorer, Microsoft Edge, Microsoft SharePoint, Windows Subsystem for Linux, Adobe Flash Player, Windows Hyper-V and Microsoft SQL Server.

CVE-201708620: Windows Search Remote Code Execution Vulnerability

The most interesting and most important vulnerability is the Windows Search Remote Code Execution Vulnerability (CVE-2017-8620), affecting all versions of Windows 7, Windows 10, which can be used to attack with computer worms like in the WannaCry case because it uses SMBv1 connection.

An attacker could exploit the vulnerability through an SMB connection to gain priority and gain control of the target Windows computer.



Many important vulnerabilities are fixed during this security update

> 'Remote code execution vulnerability occurs when Windows Search processes objects in memory. An attacker who successfully exploited this vulnerability could control the infected system. You can then install the program, view, change, delete data or create a new account with full user rights,

> "Microsoft explained. 'In addition to security changes to patch the vulnerability, this update also includes in-depth defense to help improve security-related features.

CVE-2017-8633: Windows Error Reporting Elevation of Privilege Vulnerability

Another important priority-related vulnerability in Windows Error Reporting (WER) can allow an attacker to run programs created specifically to gain administrative rights on the target machine and steal information. sensitive. 'This update will correct the way WER handles and executes files'.

CVE-2017-8627: Windows Sybsystem for Linux DoS Vulnerability

An important vulnerability discovered in Windows Subsystem for Linux allows an attacker to execute code with higher permissions.

> 'To exploit the vulnerability, an authenticated attacker can run the generated software. This security update solves the problem by correcting how Windows Subsystem for Linux NT Pipe processing.

Successful exploitation will result in refusal to attack the service, making the infected device unresponsive. Microsoft also released an important security update for Adobe Flash Player on Internet Explorer that will stop supporting Flash by the end of 2020.

To install the update, simply go to **Settings** > **Update & Security** > **Windows Update** and check for updates or manually install.