Check out some of the serious security holes that need to be fixed in the first days of 2020

The year 2020 is near, and here are particularly serious gaps that need urgent patching.

According to the statistics of the National Vulnerability Database (NVD) of the United States, on average, in 2019, there are nearly 45 new security holes discovered every day, up more than 130% compared to the first statistical point of the year. 2016.

Of the vulnerabilities found last year, 60% were rated as 'Critical' (serious) or high risk. 45% of this affects Microsoft products, which are used by billions worldwide - an alarming number.

2020 is approaching, and here are particularly serious vulnerabilities that have been reported since 2017 but so far have not received any patches:

CVE-2019-0708 - Affects old versions of Microsoft Windows

Also known as 'BlueKeep' - an unauthenticated remote code execution flaw affecting most commonly used Microsoft products such as Remote Desktop Services on Windows 7, Windows Server 2008 and Windows Server 2008 R2. This vulnerability could allow hackers to execute arbitrary code on the target system.

1. If you are using Windows 7, Windows XP, install the Microsoft BlueKeep vulnerability immediately
2. How to fix BlueKeep security errors for Windows 2003, Windows XP, Windows 7, Windows Server 2008

CVE-2019-2725 - Oracle WebLogic Server

This vulnerability, when successfully exploited, could allow a hacker to remotely execute code on the target system without authentication. It affects Oracle WebLogic Server versions 10.3.6.0 and 12.1.3.0.

CVE-2018-12130 - Intel x86 processors

The side-channel vulnerability could allow an attacker to read privileged data across trusted boundaries. Microsoft has released a software update to minimize this vulnerability, but actual exploits have been recorded so far.

CVE-2018-0802 - Microsoft Office

Classified as a remote code execution flaw, CVE-2018-080 can allow an attacker to run arbitrary code on the target system in real time, performing basic to advanced tasks such as Program settings, view, change or delete data.

CVE-2018-7600 - Drupal

The vulnerability could be misused by an attacker to execute arbitrary code, affecting Drupal versions 7.58, 8.3.9.8.4.6 and 8.5.1 and earlier.

CVE-2018-20250 - WinRAR

The flaw was seriously exploited during a targeted attack against organizations in the satellite and communications industry. An attacker can take advantage of this vulnerability to run various code execution techniques.

1. Detect code execution vulnerabilities from WinRAR, record more than 100 cases of infringement

CVE-2018-4878 - Adobe Flash Player

The vulnerability could result in remote code execution in Adobe Flash Player 28.0.0.137 and earlier versions.

CVE-2017-8570 - Microsoft Office

The vulnerability allows hackers to distribute malicious code hidden in MS documents.

CVE-2017-5715 - Specter and Meltdown

The vulnerability appears on Intel, AMD and even ARM chips that allow hackers to read sensitive information in memory, including operating systems and other programs, and even be exploited using javascript code through the program. browse when accessing the web.

Above are a few of the serious vulnerabilities that need to be addressed in the near future. What do you know about these vulnerabilities? Leave your comments below.