Warning of 16 security vulnerabilities causing Microsoft products to be attacked

The Department of Information Security (Ministry of Information and Communications) has just issued a warning about 16 security vulnerabilities with high and serious impacts in Microsoft products.

The list of security vulnerabilities in Microsoft products warned this time mainly allows attackers to execute remote code including: 3 vulnerabilities CVE-2024-21322, CVE-2024-21323, CVE2024- 29053 in 'Microsoft Defender for IoT'; CVE-2024-26256 vulnerability in the open source library Libarchive; CVE-2024-26257 vulnerability in Microsoft Excel spreadsheet; 7 vulnerabilities CVE-2024-26221, CVE-2024-26222, CVE2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231 and CVE2024-26233 in Windows DNS Server.

In particular, experts believe that two vulnerabilities need special attention, namely the vulnerability CVE-2024-20678 in Remote Procedure Call Runtime (a Windows component that facilitates communication between different processes in the system). system over the network), allowing attackers to execute remote code and the vulnerability CVE-2024-29988 in the SmartScreen security feature built into Windows, allows attackers to bypass security mechanisms. guard.

Along with that, units need to pay additional attention to two vulnerabilities that allow subjects to perform spoofing attacks (Spoofing). These are the vulnerability CVE-2024-20670 in Outlook for Windows software that exposes NTML hashes and the vulnerability CVE-2024-26234 in Proxy Driver.

The above vulnerabilities were warned by the Information Security Department on the basis of evaluation and analysis from the April 2024 patch list announced by Microsoft with 147 vulnerabilities existing in this technology company's products.

Faced with the above situation, the Department of Information Security recommends that agencies, organizations as well as businesses immediately check, review and identify computers using the Windows operating system that are likely to be affected.

At the same time, update the patch promptly to avoid the risk of cyber attacks. The goal is to ensure information security for the units' information systems, contributing to ensuring the safety of Vietnam's cyberspace.

In addition, units should strengthen monitoring and be ready with solutions when detecting signs of cyber exploitation or attack. Regularly monitor warning channels of authorities and large information security organizations to promptly detect cyber attack risks.

Security vulnerabilities are one of the leading causes of cyber attacks targeting information systems of organizations and businesses in the world and Vietnam. In particular, high-level and serious vulnerabilities, if not handled immediately, will put agencies and organizations at immediate risk of attack.

Statistics published by the Department of Information Security at the end of last year showed that more than 70% of organizations have not paid attention to reviewing and updating and patching warned vulnerabilities and weaknesses.