Users should update Windows immediately to fix 33 vulnerabilities

Microsoft has just released the final Patch Tuesday patch for 2023 to fix 33 vulnerabilities, and recommends that users update Windows immediately.

According to data from the Zero Day Initiative, Microsoft has patched more than 900 security vulnerabilities this year through Windows updates. There are no reports that these vulnerabilities have been made public or exploited in the wild, however, there are several notable vulnerabilities, including:

- **CVE-2023-35628 (CVSS score: 8.1):** Remote code execution vulnerability on Windows MSHTML platform

- **CVE-2023-35630 (CVSS score: 8.8):** Internet Connection Sharing (ICS) remote code execution vulnerability

- **CVE-2023-35636 (CVSS score: 6.5):** Microsoft Outlook information disclosure vulnerability

- **CVE-2023-35639 (CVSS score: 8.8):** Microsoft ODBC driver remote code execution vulnerability

- **CVE-2023-35641 (CVSS score: 8.8):** Internet Connection Sharing (ICS) remote code execution vulnerability

- **CVE-2023-35642 (CVSS score: 6.5):** Internet Connection Sharing (ICS) denial of service vulnerability

- **CVE-2023-36019 (CVSS score: 9.6):** Microsoft Power Platform connector spoofing vulnerability

- **CVE-2023-36019** is also important because it allows an attacker to send a specially crafted URL to a target, leading to the execution of malicious scripts in the victim's browser.

Microsoft said hackers can manipulate a malicious link, application or file to disguise it as a legitimate link or file to trick victims.

To limit attacks, users should update Windows as soon as possible by clicking on the Start menu and selecting Settings - Security & Update - Windows Update - Check for Updates.

Microsoft's final Patch Tuesday of 2023 also fixes three vulnerabilities in the DHCP server service, which could lead to denial of service or information disclosure.

- **CVE-2023-35638 (CVSS score: 7.5):** DHCP server service denial of service vulnerability

- **CVE-2023-35643 (CVSS score: 7.5):** DHCP server service information disclosure vulnerability

- **CVE-2023-36012 (CVSS score: 5.3):** DHCP server service information disclosure vulnerability

This revelation also comes as Akamai discovered a new series of attacks against Active Directory domains using Microsoft's DHCP server.

'These attacks could allow attackers to spoof sensitive DNS records, stealing credentials,' Ori David said in a report last week.

However, Microsoft says that these issues are not serious enough to receive Windows updates, and asks users to disable DHCP DNS Dynamic Updates if not necessary and not to use DNSUpdateProxy.