Alert Bulletin

Bulletin N.: 2023-09
Publication Date: 05/12/2023
Subject: Alert 2023-09 – Multiple Critical Vulnerabilities in Microsoft Products
Traffic Light Protocol (TLP): White

Critical vulnerabilities have been reported affecting Microsoft products. The company has published updates for a total of 63 issues in its **November 2023 bulletin**, including three that threat actors are actively exploiting and two that were previously disclosed but had not yet been exploited.

Among the most important vulnerabilities reported and patched by Microsoft, we can detail:

- **CVE-2023-36025** classified as critical with a CVSSv3 score of 8.8. This vulnerability specifically affects the SmartScreen component of Windows. SmartScreen is an integrated component of Windows that attempts to detect and block malicious websites and files. The vulnerability allows malicious content to bypass the SmartScreen security feature. According to Microsoft, attackers could exploit it by tricking a Windows user into clicking a malicious link to a file shortcut. The attacker could leverage this flaw by creating a malicious Internet shortcut (.URL) file and convincing a target to click on the file or a hyperlink pointing to a .URL file. A successful exploitation would result in bypassing security controls in Windows Defender SmartScreen.
- **CVE-2023-36439** classified as critical with a CVSSv3 score of 8.0. This Remote Code Execution (RCE) vulnerability would allow attackers to install malicious software on a Microsoft Exchange mail server. This vulnerability technically requires the attacker to be authenticated on the target's local network, but it is also noted that a pair of spoofed Exchange credentials would provide that same access. In this case, an authenticated attacker on a vulnerable Exchange server with a valid user could exploit this vulnerability to gain RCE as *NT AUTHORITY\SYSTEM* in the server's mailbox backend.

- Two additional vulnerabilities in Microsoft Exchange are reported: **CVE-2023-36039**, **CVE-2023-36035**, and **CVE-2023-36050**. All of these are of important severity, with a CVSSv3 score of 7.0 and are of the spoofing type. They can be exploited in conjunction with the vulnerability **CVE-2023-36439**.

Reports indicate that the RCE vulnerability affecting the Microsoft Exchange mail server is being widely exploited. We recommend taking action quickly and applying the published security patches as soon as possible.