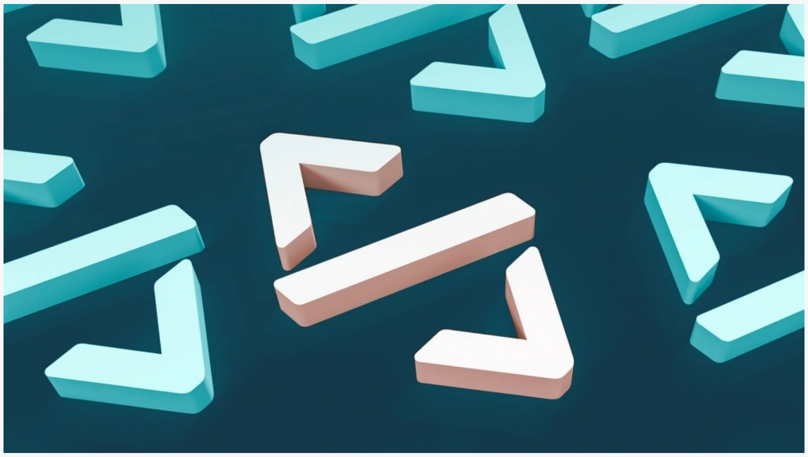
EINPRESSWIRE

ESET Research: Spy group exploits WPS Office zero day; analysis uncovers a second vulnerability



DUBAI, DUBAI, UNITED ARAB EMIRATES, September 6, 2024 /EINPresswire.com/ -- ESET researchers discovered a remote code execution vulnerability in WPS Office for Windows (CVE-2024-7262). It was being exploited by APT-C-60, a South Korea-aligned cyberespionage group, to target East Asian countries. When examining the root cause, ESET discovered another way to exploit the faulty code (CVE-2924-7263). Following a coordinated disclosure process, both vulnerabilities are now patched. The final payload in the APT-C-60 attack is a custom backdoor with cyberespionage capabilities that ESET Research internally named SpyGlace.

“While investigating APT-C-60 activities, we found a strange spreadsheet document referencing one of the group’s many downloader components. The WPS Office software has over 500 million active users worldwide, which makes it a good target to reach a substantial number of individuals, particularly in the East Asia region,” says ESET researcher Romain Dumont, who analyzed the vulnerabilities. During the coordinated vulnerability disclosure process between ESET and the vendor, DBAPPSecurity independently published an analysis of the weaponized vulnerability and confirmed that APT-C-60 has exploited the vulnerability to deliver malware to users in China.

The malicious document comes as an MHTML export of the commonly used XLS spreadsheet format. However, it contains a specially crafted and hidden hyperlink designed to trigger the execution of an arbitrary library if clicked when using the WPS Spreadsheet application. The rather unconventional MHTML file format allows a file to be downloaded as soon as the document is opened; therefore, leveraging this technique while exploiting the vulnerability provides for remote code execution.

“To exploit this vulnerability, an attacker would need to store a malicious library somewhere accessible by the targeted computer either on the system or on a remote share, and know its file path in advance. The exploit developers targeting this vulnerability knew a couple of tricks that helped them achieve this," explains Dumont. "When opening the spreadsheet document with the WPS Spreadsheet application, the remote library is automatically downloaded and stored on disk," he adds.

Since this is a one-click vulnerability, the exploit developers embedded a picture of the spreadsheet's rows and columns inside to deceive and convince the user that the document is a regular spreadsheet. The malicious hyperlink was linked to the image so that clicking on a cell in the picture would trigger the exploit.

"Whether the group developed or bought the exploit for CVE-2024-7262, it definitely required some research into the internals of the application but also knowledge of how the Windows loading process behaves," concludes Dumont.

After analyzing Kingsoft's silently released patch, Dumont noticed that it had not properly corrected the flaw and discovered another way to exploit it due to an improper input validation. ESET Research reported both vulnerabilities to Kingsoft, who acknowledged and patched them. Two high severity CVE entries were created: CVE-2024-7262 and CVE-2024-7263.

The discovery underlines the importance of a careful patch verification process and making sure that the core issue has been addressed in full. ESET strongly advises WPS Office for Windows users to update their software to the latest release.

For more technical information about the WPS Office vulnerabilities and exploits, check out the blog post "Analysis of two arbitrary code execution vulnerabilities affecting WPS Office" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here