

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

APT-C-60's 1-Click WPS Office Exploit

Date of Publication

August 29, 2024

Admiralty Code

A1

TA Number

TA2024334

Summary

First Seen: February 2024

Affected Product: WPS Office for Windows

Threat Actor: APT-C-60 (aka False Hunter, Pseudo Hunter)

Malware: SpyGlance Backdoor

Targeted Countries: China, Hong Kong, Macau, Japan, Mongolia, North Korea, South Korea, Taiwan

Impact: The South Korea-linked cyberespionage group APT-C-60 has been actively targeting East Asian organizations by exploiting a zero-day vulnerability, CVE-2024-7262, in the Windows version of WPS Office. This sophisticated attack leverages the CVE-2024-7262 flaw to deliver the SpyGlance backdoor through phishing emails. Additionally, a related security flaw, CVE-2024-7263, surfaced due to an incomplete patch addressing the initial vulnerability, leaving WPS Office users vulnerable to arbitrary code execution.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-7262	WPS Office Remote Code Execution Vulnerability	Kingsoft WPS Office for Windows	✓	✗	✓
CVE-2024-7263	WPS Office Remote Code Execution Vulnerability	Kingsoft WPS Office for Windows	✓	✗	✓

Vulnerability Details

#1

The South Korean cyberespionage group APT-C-60, also known as False Hunter or Pseudo Hunter, has exploited a zero-day vulnerability in the Windows version of WPS Office, identified as CVE-2024-7262, to deploy the SpyGlance backdoor on East Asian targets.

#2

This vulnerability, CVE-2024-7262, originates from inadequate validation of user-supplied file paths, particularly the 'ksoqing://' protocol, which permits the execution of external applications via specially crafted URLs within documents. This flaw enables adversaries to upload arbitrary Windows libraries and achieve remote code execution.

#3

APT-C-60 weaponized this vulnerability into a one-click exploit disguised as booby-trapped MHTML spreadsheet documents. These documents contain malicious hyperlinks concealed beneath a decoy image, designed to trick victims into activating the exploit.

#4

Upon execution, the processed URL parameters include a base64-encoded command that directs the execution of a specific plugin, `promcecfpluginhost.exe`, which then attempts to load a malicious DLL containing the attacker's code. This DLL serves as APT-C-60's downloader, responsible for retrieving the final payload, the custom `SpyGlance` backdoor, from the attacker's server.

#5

The group distributed these malicious documents through phishing emails related to China-ROK relations, leveraging the zero-day vulnerability to trigger the payload. Although CVE-2024-7262 was quietly patched, the fix only addressed part of the faulty code, leaving other exploitable elements intact. Additionally, a second vulnerability, CVE-2024-7263, was identified, allowing arbitrary code execution by hijacking the control flow of the WPS Office plugin component, `promcecfpluginhost.exe`.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-7262	Kingsoft WPS Office version from 12.2.0.13110 to 12.1.0.16412	<code>cpe:2.3:a:kingsoft:wps_office:*.~.*.*.*.*.*.*</code>	CWE-22
CVE-2024-7263	Kingsoft WPS Office version 12.2.0.13110 to 12.2.0.17115 (exclusive)	<code>cpe:2.3:a:kingsoft:wps_office:*.~.*.*.*.*.*.*</code>	CWE-22

Recommendations



Immediate Software Update: Upgrade to the latest version of WPS Office for Windows. The patch in version 12.1.0.17119 was insufficient; ensure you are using the most recent release to mitigate CVE-2024-7262 effectively. The initial patch did not fully address the vulnerability, leaving systems exposed. Regular updates are crucial to maintaining security.



Enhanced Email Filtering: Deploy advanced email filtering solutions to detect and block phishing emails that may contain malicious WPS Office documents. Phishing is a common vector for delivering exploits. Effective filtering can reduce the risk of initial infection.



Review and Harden Patch Management Procedures: Ensure your patch management process includes verification steps to confirm the completeness and effectiveness of patches. Incomplete or ineffective patches can leave systems vulnerable, as seen with the initial CVE-2024-7262 patch.



Regularly Review and Update Dependencies: Monitor and update any third-party integrations or dependencies used with the WPS Office. Ensure that these components are also kept up-to-date with security patches to avoid potential vulnerabilities.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery	<u>TA0040</u> Impact	<u>T1203</u> Exploitation for Client Execution
<u>T1583</u> Acquire Infrastructure	<u>T1583.001</u> Domains	<u>T1583.004</u> Server	<u>T1608</u> Stage Capabilities
<u>T1608.001</u> Upload Malware	<u>T1587</u> Develop Capabilities	<u>T1587.004</u> Exploits	<u>T1204.001</u> Malicious Link
<u>T1566</u> Phishing	<u>T1566.001</u> Spearphishing Attachment	<u>T1204</u> User Execution	<u>T1204.002</u> Malicious File
<u>T1027</u> Obfuscated Files or Information	<u>T1010</u> Application Window Discovery	<u>T1574</u> Hijack Execution Flow	<u>T1041</u> Exfiltration Over C2 Channel

🔗 Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	914cbe6372d5b7c93addc4feb5e964cd
SHA1	7509b4c506c01627c1a4c396161d07277f044ac6, 08906644b0ef1ee6478c45a6e0dd28533a9efc29
File Name	input.htm, WPS_TEST_DLL.dll
Domain	rammenale[.]com
IPv4	162[.]222[.]214[.]48, 131[.]153[.]206[.]231

🔗 Patch Details

The patch included in version 12.1.0.17119 to address CVE-2024-7262 was found to be insufficiently restrictive. To ensure comprehensive protection, WPS Office for Windows users are strongly advised to upgrade to the latest software release.

Link:

<https://www.wps.com/download/>

🔗 References

<https://www.welivesecurity.com/en/eset-research/analysis-of-two-arbitrary-code-execution-vulnerabilities-affecting-wps-office/>

<https://mp.weixin.qq.com/s/F8hNyESBdKhWxkQPgtGpew>

<https://www.wps.com/whatsnew/pc/20240422/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

August 29, 2024 • 9:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com