

CVE-2026-21509: APT28 Actively Exploits Microsoft Office Vulnerability in Ukraine

 socradar.io/blog/cve-2026-21509-apt28-microsoft-office-ukraine

Ameer Owda

February 3, 2026



On January 26, 2026, Microsoft released an update to address **CVE-2026-21509**, a high-severity vulnerability affecting nearly every modern version of Microsoft Office and the flaw is currently being exploited in the wild by state-sponsored threat actors, including the Russian-linked group **UAC-0001 (APT28)**, to target government and diplomatic organizations.

By leveraging a specially crafted document, attackers can bypass **Object Linking and Embedding (OLE)** security mitigations.

This blog explains what CVE-2026-21509 is, which versions are affected, how the attacks on Ukraine worked, what indicators defenders should look for, and what actions organizations should take next.

< CVE-2026-21509

Subscribe

Overview

News 10+

Social Media

APT Groups 4

Exploits 5

Related CVEs 26

Microsoft Office Security Flaw Opens Door for Local Attacks

A vulnerability in Microsoft Office allows attackers to bypass security features on a user's computer. By manipulating how Office handles untrusted data, a malicious user can trick the software into ignoring security protocols. This is a high-severity vulnerability, with a CVSS score of 7.8 and an SVRS score of 89, demanding immediate attention.

The Discovery

On January 26, 2026, a security flaw was disclosed in Microsoft Office. This vulnerability stems from how Office makes security decisions based on data it receives. Specifically, the software relies on user-provided input without proper validation, meaning that an attacker can craft malicious data to influence those decisions. This is known as 'Reliance on Untrusted Inputs in a Security Decision', which essentially means the software trusts data it shouldn't.

The Impact

Imagine opening a seemingly harmless Microsoft Word document or Excel spreadsheet. Embedded within this file could be specially crafted data that exploits this vulnerability. Upon opening the file, the attacker could bypass local security measures, potentially leading to unauthorized access to sensitive information or the execution of malicious code on your computer. Any user of Microsoft Office is potentially at risk. The damage could range from data theft to system compromise.

The Threat Landscape

This isn't just a theoretical risk; the vulnerability is actively being exploited in the wild, with multiple proof-of-concept exploits publicly available on platforms like GitHub. Although no specific Advanced Persistent Threat (APT) groups have been identified targeting this vulnerability, the high volume of social media mentions (26) indicates widespread awareness and interest among both security researchers and potentially malicious actors. Currently, there are no specific indicators of Compromise (IOCs) to identify compromised systems, which highlights the need for proactive patching.

The Severity & Action

With a CVSS score of 7.8, this vulnerability is classified as High severity. This means exploitation is relatively easy, and the impact on confidentiality, integrity, and availability is significant. The Socradar Vulnerability Risk Scoring (SVRS) of 89 further emphasizes the urgency. Given that exploits are already available and the vulnerability is actively being exploited ('In The Wild' tag), patching or implementing available workarounds is crucial. Immediately update your Microsoft Office installation to the latest version to mitigate this risk.

Quick Facts

This is a High severity vulnerability (CVSS 7.8), presenting an Active threat due to publicly available exploits. The vulnerability affects Microsoft Office systems. It was first seen on January 26, 2026, and last updated on January 27, 2026. Given that CISA KEV tag is present, US Federal Civilian Executive Branch agencies are required to remediate this vulnerability.

CVSS v3.1 Analysis

Base Score

7.8

Attack Vector (AV)

LOCAL

Attack Complexity (AC)

LOW

Privileges Required (PR)

NONE

User Interaction (UI)

REQUIRED

Scope (S)

UNCHANGED

CVSSv3

7.8 / 10

EPSS

2.9 / 100

SVRS

89 / 100

Published Date

2026-01-26

Modified Date

2026-01-27

Plugin

Not Available

Vector String

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A/H

Tags

CISA KEY

In The Wild

Resources

rdn.rst.gov

Affected Software

Microsoft 365 Apps

Microsoft Office

Microsoft Office Long Term Servicing Channel

Details of CVE-2026-21509 (SOCRadar Vulnerability Intelligence)

How Is This Vulnerability Exploited in Real Life?

Based on the most recent intelligence, **CVE-2026-21509 (CVSS 7.8)** is actively exploited in real-world scenarios through **social engineering** campaigns. Attackers use specially crafted Microsoft Office documents to bypass security features and deploy malware.

1/6

The most detailed case study currently available involves the threat actor **UAC-0001** ([APT28](#)) targeting organizations in Ukraine.

Upgrade your plan for a targeted cybersecurity

15000 Threat Search Credits /
1000 Malware Analysis Credits and more...

[View plans](#)

Social Engineering as The Attack Vector

Because this vulnerability requires user interaction, exploitation begins with phishing or lure documents rather than automated [remote attacks](#).

Delivery Method: Attackers send phishing emails disguised as legitimate correspondence. For example, emails were sent to Ukrainian central executive bodies purporting to be from the Ukrainian Hydrometeorological Center.

Malicious Files: Victims are tricked into opening Microsoft Word documents (DOC files). Observed filenames include:

- BULLETEN_H.doc
- Consultation_Topics_Ukraine(Final).doc (related to EU/COREPER consultations)

Technical Execution Chain

Once a victim opens the malicious file, the exploit triggers a multi-stage infection process. The following kill chain was observed by CERT-UA in attacks against Ukrainian and EU targets:

1. **Initial Connection (WebDAV):** Opening the document triggers a network connection to an external server using the **WebDAV protocol**, followed by downloading a file with a shortcut file name containing program code designed to download and run the executable file.
1. **System Modification:** The exploit drops several files locally, including:
 - EhStoreShell.dll: A malicious library disguised as a legitimate storage extension.
 - SplashScreen.png: An image file containing hidden shellcode.
1. **COM Hijacking:** The attacker modifies the Windows Registry for a specific CLSID ({D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}). This technique, known as **COM hijacking**, forces the system to load the malicious DLL instead of the legitimate one.
1. **Execution Trigger:** A scheduled task named “OneDriveHealth” is created. This task terminates and restarts the explorer.exe process. When Explorer restarts, the COM hijacking ensures the malicious EhStoreShell.dll is loaded.
1. **Final Payload:** The DLL executes the shellcode hidden in the PNG file, which launches the **COVENANT** framework.

In these specific real-world attacks, the attackers utilized legitimate cloud infrastructure to hide their activity. The COVENANT framework was configured to use **Filen (filen.io)**, a legitimate [encrypted](#) cloud storage service, for its management infrastructure.

Which Versions Are Affected?

CVE-2026-21509 affects a wide range of Microsoft Office products and both **32-bit (x86)** and **64-bit (x64)** architectures are vulnerable. According to [Microsoft](#) and security researchers, the following versions are affected:

- Microsoft 365 Apps for Enterprise
- Microsoft Office LTSC 2024
- Microsoft Office LTSC 2021
- Microsoft Office 2019
- Microsoft Office 2016

Who Is Actually at Risk From This Issue?

The exposure from CVE-2026-21509 affects two broad groups. One group includes organizations that are already being targeted in active campaigns. The other includes any organization running the affected software without the patch.

1. High-Priority Targets

Ongoing campaigns show targeted delivery of lure documents tied to political and diplomatic themes.

The activity is linked to a known threat actor with a history of espionage operations.

The targeting pattern focuses on institutions involved in governance, policy, and international coordination.

2. Broader Organizational Risk

While current attacks are targeted, the vulnerability affects a massive user base. Any organization using **Microsoft Office** that has not applied the update is at risk.

Lagging Security: Security researchers predict that the number of attacks will increase in the near future due to the “inertia” of the update process, meaning organizations that are slow to patch will become easy targets for cybercriminals adopting these techniques.

3. The Human Element

You are at risk if you can be convinced to open a malicious Office file.

The exploit is delivered via [phishing](#) emails that mimic legitimate sources. Therefore, employees who frequently handle external email attachments without strict verification can be the entry point.

What Should They Do Now?

The immediate priority for any organization using Microsoft Office is to **apply the out-of-band security updates released by Microsoft**.

Here is the prioritized checklist of actions organizations should take now:

Patch Immediately

Reinforce User Training

- **Alert Users:** Warn employees about opening files from external sources, even if they appear to come from legitimate bodies.
- **Verify Senders:** Remind staff to verify the sender’s identity through a secondary channel before opening unexpected attachments.

Registry Hardening

If immediate patching is impossible, Microsoft [recommends](#) specific Windows registry modifications to reduce the attack surface.

Indicators of Compromise

You can find the IoCs published by the [CERT-UA](#) below.

Files:

7c396677848776f9824ebe408bbba943

c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f

BULLETTEN_H.doc

d8e880975ab01c745386663409a9d3aab2e771cbfa0a74d0774db162d28c1eecd3a7cb384dfe97522e9baabd1c04d304
document.doc.Lnk

744bbe8d7c3d0421fa0deb582481f5ba

8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9

s.d

4423b8f3456e54eb48dfbde0b4c7984b

52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b7598

EhStoreShell.dll

418dc7365e78f79ef7dfcfbfe1bc8b0ec4389cc34b672c4f885547f413bf38575e6ee2b23a0ddfd306a69c1775db6fc

SplashScreen.png

331e055e6a519d443233bd740dbfe8ee495cf3fd22d4fc2c6c86b689b68141ac7d0130b0bb5cbc834ef59275132ee5c2

SplashScreen_shellcode.bin

6f528ad405bffa4a8c2f61b1fa2172fd

40c2e559992a7f595c593b419930a3f216516c3042ad86fb985348d53b6e01b9

covenant.dll (COVENANT)

ee0b44346db028a621d1dec99f429823

9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8

office.xml

4727582023cd8071a6f388ea3ba2feaa

5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02

4727582023cd8071a6f388ea3ba2feaa.doc

95e59536455a089ced64f5af2539a449

b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546

Consultation_Topics_Ukraine(Final).doc

d47261e52335b516a777da368208ee91

fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b

1291.doc

b6a86f44d0a3fa5a5ac979d691189f2d

969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae

1301.doc

Network:

- (smb)://freefoodaid[.]com/documents/template_2_2.doc
- (smb)://wellnesscared[.]com/davwwwroot/buch/Downloads/blank.doc
- (smb)://wellnesscared[.]com/davwwwroot/venezia/Favorites/blank.doc
- (smb)://wellnessmedcare[.]org@ssl/cz/Downloads/blank.doc
- (smb)://wellnessmedcare[.]org@ssl/pol/Downloads/blank.doc
- hXXp://freefoodaid[.]com/davwwwroot/2_2.Lnk?init=
- hXXp://freefoodaid[.]com/documents/2_2.Lnk?init=
- hXXps://wellnesscared[.]com/buch/Downloads/document.doc.Lnk?init=
- hXXp://wellnesscared[.]com/buch/Downloads/document.doc.Lnk?init=
- hXXp://wellnesscared[.]com/venezia/Favorites/document.doc.Lnk?init=
- hXXp://wellnesscared[.]com/venezia/d/s.d
- hXXps://wellnessmedcare[.]org/davwwwroot/cz/Downloads/document.Lnk?init=
- hXXp://wellnessmedcare[.]org/davwwwroot/cz/Downloads/document.Lnk?init=
- hXXps://wellnessmedcare[.]org/davwwwroot/pol/Downloads/document.Lnk?init=
- hXXp://wellnessmedcare[.]org/davwwwroot/pol/Downloads/document.Lnk?init=

- freefoodaid[.]com (2026-01-12)
- wellnesscared[.]com (2026-01-12)
- wellnessmedcare[.]org (2026-01-30)

- 159[.]253.120.2
- 193[.]187.148.169
- 23[.]227.202.14

File cloud storage infrastructure:

- *.filen.net
- *.filen-1.net
- *.filen-2.net
- *.filen-3.net
- *.filen-4.net
- *.filen-5.net
- *.filen-6.net
- *.filen.io
- *.filen.dev

- 146.0.41.204
- 146.0.41.205
- 146.0.41.206
- 146.0.41.207
- 146.0.41.208

146.0.41.231

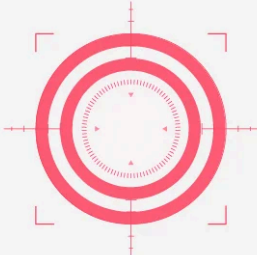
146.0.41.232

146.0.41.233

146.0.41.234

Host:

- %PROGRAMDATA%\Microsoft OneDrive\setupCache\SplashScreen.png
- %PROGRAMDATA%\USOPublicData\UserEhStore\Shell.dll
- %TMP%\Diagnosticsoffice.xml
- HKCU\Software\Classes\CLSID{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32'(Default)'
- HKCU\Software\Classes\CLSID{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}\InProcServer32'\ThreadingModel'
- schtasks /delete /f /tn OneDriveHealth
- schtasks.exe /Create /tn "OneDriveHealth" /XML "%TMP%\Diagnosticsoffice.xml"
- start explorer >nul 2>&1
- taskkill /f /IM explorer.exe >nul 2>&1
- OneDriveHealth



Cyber Threat Intelligence

*Your Shield Against Cyber Adversaries
is even stronger now!*

[→ Get Free Access](#)