

# Inside the Fix: Analysis of In-the-Wild Exploit of CVE-2026-21513

 [akamai.com/blog/security-research/2026/feb/inside-the-fix-cve-2026-21513-mshtml-exploit-analysis](https://akamai.com/blog/security-research/2026/feb/inside-the-fix-cve-2026-21513-mshtml-exploit-analysis)

## Component

---

ieframe.dll (MSHTML/IEFrame navigation + protocol launching path).

## Vulnerability Class

---

Protection Mechanism Failure (CWE-693). Security feature bypass in the protocol-launch (ShellExecute) decision logic for hyperlink navigation

## Detailed Root Cause Analysis

---

The vulnerable behavior is in `_AttemptShellExecuteForHlinkNavigate()`, which takes an input URL (`a1, WCHAR*`) and decides whether to invoke `ShellExecuteExW()` on that URL (after percent-encoding) and sets an out-parameter flag (`a2`) indicating `ShellExecute` was attempted.

Before the patch, once the scheme name was parsed (`CreateUri + IUri::GetSchemeName`) and validated (`IsValidSchemeName`), the function only applied a single policy gate:

```
v5 = !ShouldDisableIEShellExecuteProtocol(pbstr);
```

If `v5` was true, it would percent-encode the original URL into a fixed stack buffer (`v11[2088]`) using `PrepareURLWithPercentEncoding()`, then unconditionally call `ShellExecuteExW()` with `lpFile` pointing at that buffer.

## Executive summary

---

- On February 2026's Patch Tuesday, Microsoft patched **CVE-2026-21513**, a security features bypass vulnerability within MSHTML framework.

- The vulnerability affects all Windows versions, is actively exploited in the wild, and carries a **CVSS score of 8.8**.
- Using **PatchDiff-AI**, Akamai researchers performed automated root cause analysis of the patch and correlated it with an observed in-the-wild exploit attributed to the **Russian state-sponsored threat actor APT28**.
- This blog post provides a technical breakdown of CVE-2026-21513, a description of its root cause, and an analysis of its exploitation.
- We have included a list of indicators of compromise (IOCs) in this blog post to assist in defense against this threat.

## The vulnerability

---

Microsoft's February 2026 Patch Tuesday addressed 59 vulnerabilities, including six actively exploited [zero-days](#). CVE-2026-21513 stands out because of its [active exploitation](#), high impact, and ability to bypass browser security boundaries and trigger arbitrary file execution.

We used the multi-agent system called [PatchDiff-AI](#) to analyze [CVE-2026-21513](#) and its patch. PatchDiff-AI generated a detailed report that reveals insights about the vulnerable component and the attack vector.

## The root cause

---

The report by PatchDiff-AI ties CVE-2026-21513 to a specific function within **ieframe.dll** (Internet Explorer frame). The vulnerability resides in the logic responsible for handling hyperlink navigation. Insufficient validation of the target URL allows attacker-controlled input to reach code paths that invoke **ShellExecuteExW**, enabling execution of local or remote resources outside the intended browser security context (Figure 1).

Fig. 1: Snippet from PatchDiff-AI report, pinpointing the vulnerable code path

The code path visualization in Figure 2 shows flow differences in the function `_AttemptShellExecuteForHlinkNavigate` applied by the patch.

Fig. 2: PatchDiff-AI compares the vulnerable function before and after the patch

To trigger the vulnerable code block, we needed to invoke Internet Explorer using an ActiveX form to track down what exactly initiates the flow. Using the component of "System.Windows.Forms.WebBrowser" and displaying it on the "System.Windows.Forms.Form" object, we loaded an HTML file that was parsed and constructed using the MSHTML and IFRAME modules.

Another important component is the "htmlfile," which exposes the DOM interface and allows us to manipulate it in a way that will trigger the vulnerable function.

While exploring the vulnerable code and the function calls that trigger it, we were led to the following exploit.

## The exploit

---

By correlating the vulnerable code path with public threat intelligence, we identified a sample that was leveraging this functionality: document.doc.LnK.download.

The sample was first submitted to VirusTotal on January 30, 2026, shortly before February's Patch Tuesday, and is associated with infrastructure linked to APT28, [an active Russian state-sponsored threat actor](#) (Figure 3).

Fig. 3: A VirusTotal screenshot of APT28's exploit

This payload involves a specially crafted Windows Shortcut (.lnk) that embeds an HTML file immediately after the standard LNK structure.

The LNK file initiates communication with the domain wellnesscaremed[.]com, which is attributed to APT28 and has been in extensive use for the campaign's multistage payloads.

The exploit leverages **nested iframes and multiple DOM contexts** to manipulate trust boundaries.

This technique allows the attacker to **bypass Mark of the Web (MotW) and Internet Explorer Enhanced Security Configuration (IE ESC)**, effectively downgrading the security context before triggering the vulnerable navigation flow. Ultimately, this allows attacker-controlled content to reach a code path that invokes **ShellExecuteExW**, leading to execution outside of the browser sandbox (Figure 4).

```
{ h1 = new window[0].ActiveXObject('htmlfile'); };
('<html><body><iframe src=%22about:blank%22></iframe><iframe src=%22about:blank%22>
</iframe>%3cscript
defer%3ewindow[1].document.Script.open(%22http:///%22,%22_parent%22)%3c/script%3e</body>
</html>');
```

Fig. 4: A call to the vulnerable code block using the “document.Script.open()” method

If we run this script in Internet Explorer directly, we will encounter the security feature mentioned above, which warns the user and reduces the chances for successful exploitation (Figure 5).

Fig. 5: A user warning before the script is executed

Successful exploitation will bypass the security features and execute code controlled by the attacker. The screenshot in Figure 6 shows the top of the call stack, a very long one, where we can see the call to the vulnerable function `_AttemptShellExecuteForHlinkNavigate`.

Fig. 6: The call stack during exploitation

While the observed campaign leverages malicious **.LNK files**, the vulnerable code path can be triggered through any component embedding MSHTML. Therefore, additional delivery mechanisms beyond LNK-based [phishing](#) should be expected.

## The fix

Microsoft introduced stricter validation to the hyperlink protocol that ensures supported protocols (such as file://, http://, and https://) will execute within the browser context rather than being passed directly to [ShellExecuteExW](#).

## Protecting your assets

Applying Microsoft's [February 2026 security updates](#) fully mitigates this vulnerability.

APT28's domains are tracked in Akamai's proprietary threat intelligence. [Akamai Hunt](#) detects and alerts on activity patterns associated with this attack [[T1204.001](#), [T1566.001](#)], and automatically notifies customers when vulnerable assets are detected.

PatchDiff-AI quickly analyzes the root cause of a vulnerability, enabling rapid root cause identification of vulnerabilities and accelerating analysis of in-the-wild exploitations.

[Learn more at RSAC 2026](#)

## IOCs

| Name             | Indicator                                                      |
|------------------|----------------------------------------------------------------|
| document.doc.LnK | aefd15e3c395edd16ede7685c6e97ca0350a702ee7c8585274b457166e86b' |
| Domain           | wellnesscaremed[.]com                                          |
| MITRE Techniques | T1204.001, T1566.001                                           |

[Read more research](#)



Written by

[Maor Dahan](#)

Maor Dahan is a Senior Security Researcher at Akamai with more than a decade of experience in the cybersecurity industry. He specializes in operating system internals, vulnerability research, and malware analysis. Maor also has extensive experience designing and developing advanced detection and prevention mechanisms for innovative security products such as EDR, EPP, and virtualization-based security.

Tags

- [Cyber Security](#)
- [Research](#)
- [Security Research](#)
- [Akamai Hunt](#)

Share

## Related Blog Posts

---



[On February 6, 2026, a full fix was deployed, completely eliminating the vulnerability from all Akamai services.](#)

Security Research

CVE-2026-26365: Incorrect processing of "Connection: Transfer-Encoding"

February 20, 2026

[Akamai InfoSec](#)

Read how Akamai eliminated a potential HTTP request smuggling vector due to a bug in the processing of custom hop-by-hop HTTP headers.

[Read blog](#)



[A new rule within Akamai App & API Protector has been deployed to protect our customers from this DoS threat.](#)

Security Research

CVE-2026-23864: React and Next.js Denial of Service via Memory Exhaustion

January 26, 2026

[Akamai Security Intelligence Group](#)

A newly disclosed vulnerability that affects multiple React-based frameworks reveals a denial-of-service flaw.

[Read blog](#)



[We used cutting-edge AI-driven reverse engineering tools to discover a new vulnerability that's impacting dozens of legacy camera models.](#)

Security Research

Command Injection in Vivotek Legacy Firmware: What You Need to Know

January 20, 2026

[Larry Cashdollar](#)

Stay ahead with the latest on the Vivotek upload\_map.cgi vulnerability, CVE-2026-22755, and protect your legacy firmware from command injection attacks.

[Read blog](#)

Rate the helpfulness of this page

- [Cloud Computing](#)
- [Security](#)
- [Content Delivery](#)
- [All Products and Trials](#)
- [Global Services](#)
  
- [About Us](#)
- [History](#)
- [Leadership](#)
- [Facts and Figures](#)

- [Awards](#)
- [Board of Directors](#)
- [Infrastructure for Innovation](#)
- [Investor Relations](#)
- [Corporate Responsibility](#)
- [Ethics](#)
- [Locations](#)
- [Vulnerability Reporting](#)
- [Accessibility Statement](#)
  
- [Careers](#)
- [Working at Akamai](#)
- [Students and Recent Grads](#)
- [Workplace Diversity](#)
- [Search Jobs](#)
- [Culture Blog](#)
  
- [Newsroom](#)
- [Press Release](#)
- [In the News](#)
- [Media Resources](#)
  
- [Legal](#)
- [Information Security Compliance](#)
- [Privacy Trust Center](#)
- [Privacy Statement](#)
- [Cookie Settings](#)
- [EU Digital Services Act \(DSA\)](#)
  
- [What Is API Security?](#)
- [What Is a CDN?](#)
- [What Is Cloud Computing?](#)
- [What Is Cybersecurity?](#)
- [What Is a DDoS attack?](#)
- [What Is Microsegmentation?](#)
- [What Is WAAP?](#)
- [What Is Zero Trust?](#)
- [See all](#)

## Your cookie choices and AI settings for this website

---

We use cookies to ensure the fast reliable and secure operation of this website, to improve your website experience, to enable certain social media interactions and to manage your cookie

choices. Some cookies process personal identifiable information. By continuing to visit our websites you are agreeing to our use of cookies. Click “Manage Preferences” to make individual choices and get details on the cookies in use and the processing activities. You can access the Cookie Management Page at any time via the Cookie Settings link in the footer. For additional information relating to your privacy take a look at our [Privacy Statement](#)