

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Windows Shortcut Exploit Abused in Widespread APT Campaigns
Tracking #:432316995
Date:20-03-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability in Windows shortcut (.lnk) files, identified as ZDI-CAN-25373, is being actively exploited by multiple state-sponsored and cybercriminal groups.

TECHNICAL DETAILS:

A critical vulnerability in Windows shortcut (.lnk) files, identified as ZDI-CAN-25373, is being actively exploited by multiple state-sponsored and cybercriminal groups. This vulnerability allows attackers to execute hidden malicious commands on victims' machines through crafted shortcut files. Nearly 1,000 malicious .lnk files abusing this vulnerability have been identified.

Exploitation Techniques

Attackers exploit this vulnerability by:

1. Crafting malicious .lnk files with padded whitespace characters in the `COMMAND_LINE_ARGUMENTS` structure.
2. Hiding malicious arguments from user view in the Windows UI.
3. Using large file sizes (up to 70.1MB) to evade detection

Affected Sectors

- **Sectors:** Government, Financial, Telecommunications, Military, Energy, Think Tanks, and NGOs

APT Groups and Motivations

- 11 state-sponsored groups identified, with North Korea being the most active.
- Primary motivations: 70% espionage and information theft, 20% financial gain.

Malware Payloads

Various malware payloads and loaders have been observed in campaigns exploiting ZDI-CAN-25373, including Malware-as-a-Service (MaaS) and commodity malware


Technical Details

- The vulnerability relates to the MS-SHLLINK (.lnk) file format.
- Exploitation involves manipulating the ShellLinkHeader, LinkFlags, LinkTargetIDList, `COMMAND_LINE_ARGUMENTS`, and `ICON_LOCATION` structures.
- Whitespace characters (e.g., Space, Horizontal Tab, Line Feed) are used to pad the `COMMAND_LINE_ARGUMENTS` structure.

Impact

The exploitation of ZDI-CAN-25373 poses significant risks of data theft and cyber espionage to affected organizations. The widespread abuse by multiple APT groups underscores the severity of this vulnerability and the need for immediate action to mitigate its impact

Indicators of Compromise (IOCs):

Attached File 

RECOMMENDATIONS:

1. Immediate Security Actions:

- Scan and audit all systems for the presence of suspicious .lnk files.
- Enable endpoint protection and behavior-based threat detection.

2. Mitigation Strategies:

- Block execution of .lnk files from untrusted sources using Group Policy.
- Deploy Windows security policies to restrict command-line argument execution within shortcut files.
- Use third-party forensic tools to inspect .lnk files for hidden command-line arguments.

3. Detection and Response:

- Monitor network traffic for indicators of compromise (IOCs) related to ZDI-CAN-25373.
- Implement Security Information and Event Management (SIEM) rules to flag suspicious shortcut file activity.
- Conduct threat-hunting exercises to identify potential exploitation attempts within the environment.

4. User Awareness and Training:

- Educate employees on the risks of interacting with unknown shortcut files.
- Encourage verification of file extensions and icons before execution.
- Restrict user privileges to minimize the impact of successful exploits.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zero-day-exploit.html