A New Zero-Day Vulnerability Exploited in the wild – ClearSky Cyber Security

Published: 2024-11-13 · Archived: 2026-04-05 12:35:36 UTC

A new zero-day vulnerability, **CVE-2024-43451**, was discovered by ClearSky Cyber Security in June 2024. This vulnerability affects Windows systems and is being actively exploited in attacks against Ukrainian entities.

The vulnerability **activates URL files containing malicious code through seemingly innocuous actions**:

- A single right-click on the file (all Windows versions).
- Deleting the file (Windows 10/11).
- Dragging the file to another folder (Windows 10/11 and some Windows 7/8/8.1 configurations).

The malicious URL files were disguised as academic certificates and were initially observed being distributed from a compromised official Ukrainian government website.

Exploitation Process:

The attack begins with a phishing email sent from a compromised Ukrainian government server. The email prompts the recipient to renew their academic certificate. The email contains a malicious URL file. When the user interacts with the URL file by right-clicking, deleting, or moving it, the vulnerability is triggered. This action establishes a connection with the attacker’s server and downloads further malicious files, including SparkRAT malware.

SparkRAT is an open-source remote access trojan that allows the attacker to gain control of the victim’s system. The attackers also employed techniques to **maintain persistence** on the infected system, ensuring their access even after a reboot.

Attribution:

CERT-UA linked this campaign to the threat actor **UAC-0194**, suspected to be Russian. ClearSky also noted similarities with previous campaigns by other threat actors, suggesting the use of a common toolkit or technique.

Remediation:

Microsoft released a **security patch** for this vulnerability on November 12, 2024. Users are strongly advised to update their Windows systems to mitigate the risk posed by CVE-2024-43451.

Read the full report:
