QakBot attacks with Windows zero-day (CVE-2024-30051)

By Boris Larin

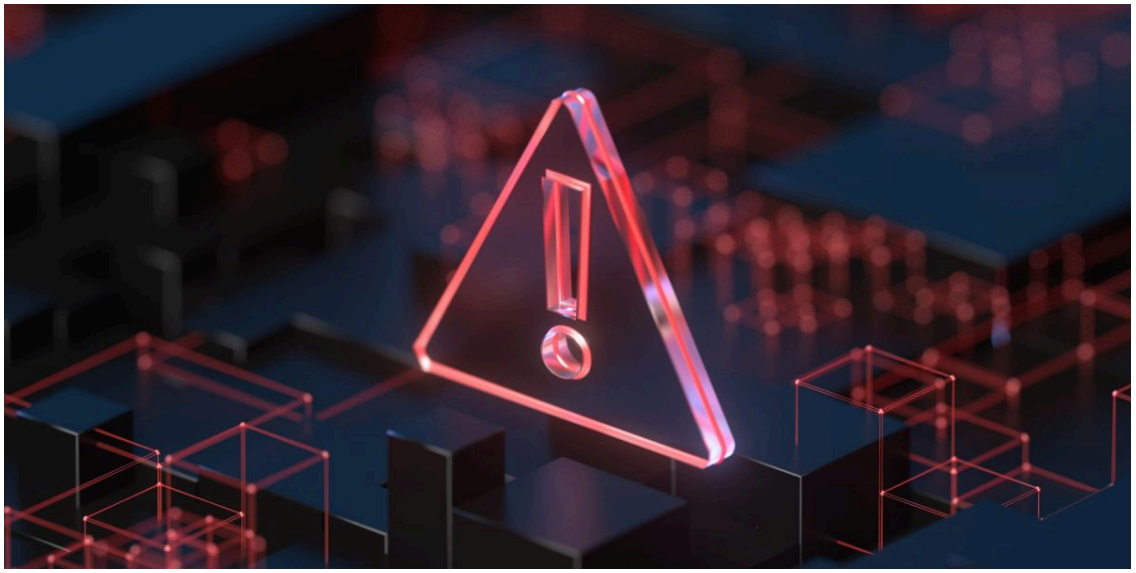
Published: 2024-05-14 · Archived: 2026-04-05 14:27:07 UTC

Software

Software

14 May 2024

1 minute read



In early April 2024, we decided to take a closer look at the Windows DWM Core Library Elevation of Privilege Vulnerability CVE-2023-36033, which was previously discovered as a zero-day exploited in the wild. While searching for samples related to this exploit and attacks that used it, we found a curious document uploaded to VirusTotal on April 1, 2024. This document caught our attention because it had a rather descriptive file name, which indicated that it contained information about a vulnerability in Windows OS. Inside we found a brief description of a Windows Desktop Window Manager (DWM) vulnerability and how it could be exploited to gain system privileges, everything written in very broken English. The exploitation process described in this document was identical to that used in the previously mentioned zero-day exploit for CVE-2023-36033, but the vulnerability was different. Judging by the quality of the writing and the fact that the document was missing some important details about how to actually trigger the vulnerability, there was a high chance that the described vulnerability was completely made up or was present in code that could not be accessed or controlled by attackers. But we still decided to investigate it, and a quick check showed that this is a real zero-day vulnerability that can be used to escalate privileges. We promptly reported our findings to Microsoft, the vulnerability was designated CVE-2024-30051, and a patch was released on May 14, 2024, as part of Patch Tuesday.

After sending our findings to Microsoft, we began to closely monitor our statistics in search of exploits and attacks that exploit this zero-day vulnerability, and in mid-April we discovered an exploit for this zero-day vulnerability. We have seen it used together with QakBot and other malware, and believe that multiple threat actors have access to it.

We are going to publish technical details about CVE-2024-30051 once users have had time to update their Windows systems.

Kaspersky products detect the exploitation of CVE-2024-30051 and related malware with the verdicts:

- PDM:Exploit.Win32.Generic;
- PDM:Trojan.Win32.Generic;
- UDS:DangerousObject.Multi.Generic;
- Trojan.Win32.Agent.gen;
- Trojan.Win32.CobaltStrike.gen.

Kaspersky would like to thank Microsoft for their prompt analysis of the report and patches.

Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
