



Zero-day Exploit in Desktop Window Manager

CRITICALITY 

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Microsoft released an update to plug a zero-day vulnerability (CVE-2021-28310) that's being exploited in active attacks already. The flaw allows an attacker to elevate their privileges on a target system.



Threat Details

This zero-day vulnerability (CVE-2021-28310) is a privilege escalation exploit (EoP) that is used in combination with other browser exploits to escape sandboxes and to obtain system privileges for further access.

It is an out-of-bounds (OBB) write vulnerability in `dwmcore.dll`, which is part of Desktop Window Manager (`dwm.exe`). Due of the lack of bounds checking, attackers may establish a scenario in which they can write controlled data at a controlled offset using the `DirectComposition` API.

`DirectComposition` API is implemented by the `win32kbase.sys` driver and the names of all associated syscalls begin with the string “`NtDComposition`” as shown in (Figure 1).

A screenshot of a list of syscalls from the `win32kbase.sys` driver. The list is displayed on a dark background with yellow text. Each line starts with 'dq offset' followed by a syscall name. The syscalls listed are: `NtDCompositionAddCrossDeviceVisualChild`, `NtDCompositionAddVisualChild`, `NtDCompositionBeginFrame`, `NtDCompositionCommitChannel`, `NtDCompositionConfirmFrame`, `NtDCompositionConnectPipe`, `NtDCompositionCreateAndBindSharedSection`, `NtDCompositionCreateChannel`, `NtDCompositionCreateConnection`, `NtDCompositionCreateDwmChannel`, `NtDCompositionCreateResource`, `NtDCompositionCurrentBatchId`, `NtDCompositionDestroyChannel`, `NtDCompositionDestroyConnection`, `NtDCompositionDiscardFrame`, `NtDCompositionDuplicateHandleToProcess`, `NtDCompositionDwmSyncFlush`, `NtDCompositionConnectPipe`, `NtDCompositionGetConnectionBatch`, `NtDCompositionGetDeletedResources`, `NtDCompositionGetFrameLegacyTokens`, `NtDCompositionGetFrameStatistics`, `NtDCompositionGetFrameSurfaceUpdates`, and `NtDCompositionOpenSharedResource`.

```
dq offset NtDCompositionAddCrossDeviceVisualChild
dq offset NtDCompositionAddVisualChild
dq offset NtDCompositionBeginFrame
dq offset NtDCompositionCommitChannel
dq offset NtDCompositionConfirmFrame
dq offset NtDCompositionConnectPipe
dq offset NtDCompositionCreateAndBindSharedSection
dq offset NtDCompositionCreateChannel
dq offset NtDCompositionCreateConnection
dq offset NtDCompositionCreateDwmChannel
dq offset NtDCompositionCreateResource
dq offset NtDCompositionCurrentBatchId
dq offset NtDCompositionDestroyChannel
dq offset NtDCompositionDestroyConnection
dq offset NtDCompositionDiscardFrame
dq offset NtDCompositionDuplicateHandleToProcess
dq offset NtDCompositionDwmSyncFlush
dq offset NtDCompositionConnectPipe
dq offset NtDCompositionGetConnectionBatch
dq offset NtDCompositionGetDeletedResources
dq offset NtDCompositionGetFrameLegacyTokens
dq offset NtDCompositionGetFrameStatistics
dq offset NtDCompositionGetFrameSurfaceUpdates
dq offset NtDCompositionOpenSharedResource
```

Figure 1: `DirectComposition` syscalls in the `win32kbase.sys` driver

Just three syscalls are needed for exploitation, which are:

- `NtDCompositionCreateChannel`:
- `NtDCompositionProcessChannelBatchBuffer`
- `NtDCompositionCommitChannel`

In summary, `NtDCompositionCreateChannel` initiates a channel that can be used together with `NtDCompositionProcessChannelBatchBuffer` syscall to send multiple `DirectComposition` commands in one go for processing by the kernel in a batch mode.



The entire process for the exploitation is as follows:

- 1- Create a vast number of resources with properties of specific size to get heap into predictable state.
- 2- Create additional resources with properties of specific size and content to spray memory at specific locations with fake properties.
- 3- Release resources created at the previous stage.
- 4- Create additional resources with properties. These resources will be used to perform OOB writes.
- 5- Make holes among resources created at the first stage.
- 6- Create additional properties for resources created at the fourth stage. Their buffers are expected to be allocated at specific locations.
- 7- Create “special” properties to cause inconsistency between the number of properties assigned to the same resource in kernel mode/user mode for resources created at the fourth stage.
- 8- Use OOB write vulnerability to write shellcode, create an object and get code execution.
- 9- Inject additional shellcode into another system process.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks

References

- April 2021 Update Tuesday packages now available.* (2021, April 13). Retrieved from Microsoft Security Response Center: <https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/>
- Critical Patches Issued for Microsoft Products, April 13, 2021.* (2021, April 13). Retrieved from Center for Internet Security: https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-april-13-2021_2021-046/
- Laren, B. (2021, April 13). *Zero-day vulnerability in Desktop Window Manager (CVE-2021-28310) used in the wild.* Retrieved from Securelist English Global securelistcom: <https://securelist.com/zero-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/>
- Microsoft's April update patches 114 bugs-half of which allow remote code execution.* (2021, April 13). Retrieved from Sophos: <https://news.sophos.com/en-us/2021/04/13/microsofts-april-update-patches-114-bugs-more-than-half-of-which-allow-remote-code-execution/>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to follow the below steps:

- Applying appropriate patches provided by Microsoft to vulnerable systems immediately.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the principle of least privilege to all the systems and services.



Appendix B – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix C – TLP Definitions

TLP:RED = Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN = Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE = Disclosure is not limited.

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.