SUMMARY

of

What we know about "aPAColypse now"

Issued : 19/12/17 at 08h15 GMT+1 by Hacknowledge

INTRODUCTION

- New set of vulnerabilities impacting Windows javascript library discovered by Google project zero
- Could be remotely exploited by providing a malicious PAC file containing javascript to vulnerable versions of Internet Explorer
- PAC files are usually provided by your internal proxy, however if your browsers are configured to perform WPAD requests, it is possible for a local attacker to spoof the WPAD answer and provide malicious javascript. This spoofing is performed through ARP spoofing or by racing the legitimate WPAD server
- Vector : local network (ARP spoofing, DNS/NetBios racing), Internet (misconfigured DNS settings on clients)

DON'T ❌

-Shutdown your WPAD server or remove it's DNS entry : clients will still perform WPAD queries until configured otherwise

DO 👍

- install the updates provided in Microsoft monthly security updates from the 12.12.17
- **disable WPAD by setting the following registry key through a GPO: HKLM\SYSTEM\CurrentControlSet\Services\WinHttpAutoProxySvc = 4 (disabled)**

Hacknowledge reaction

- we are already monitoring WPAD requests and will inform you of any suspicious requests
- we will deploy signatures to detect exploitation attempts on the monitored networks (non-TLS)

Sources

[1] https://googleprojectzero.blogspot.ch/2017/12/apacolypse-now-exploiting-windows-10-in_18.html-

[2] https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/c383fa60-b852-e711-80dd-000d3a32f9b6

Hacknowledge