CYB 240 Project One

Southern New Hampshire University

Douglas Few

2/13/2022

Server-Side Vulnerability

The vulnerability that I’ve identified on the Windows server is a PHP Denial of Service vulnerability. This vulnerability allows attackers to perform a denial of service attack, effectively overloading the server and shutting it down. Denial of service attacks are relatively common throughout the industry. Famously, GitHub experienced a distributed denial of service attack in 2018 that was caused by an exploit of a program called Memcached. Memcached is used by websites and database operators as a method of speeding up website and network traffic, but an exploited command line was able to shut down the website for approximately 20 minutes (Security Boulevard, 2020).

This vulnerability can be remedied by updating to a more recent version of PHP. In later versions, this exploit has been patched out and will no longer occur. However, it is recommended that frequent testing still occurs because new exploits and methods are discovered regularly.

Non-Server Vulnerability

On the client side, there were several end of life vulnerabilities discovered regarding PHP, OpenSSL, and Apache. An end of life vulnerability occurs when a product being used is no longer supported by that product’s developer. This can result in issues where exploits and vulnerabilities in software are found, but patches are no longer being released.

Ravie Lakshmanan with TheHackerNews.com reported on ransomware attacks targeting end of life VPN software produced by SonicWall (2021). SonicWall became aware of attacks targeting unpatched versions of their software and attempted to alert users of the risks of continuing to use outdated end of life software. The developers urged customers to upgrade to more recent versions in order to avoid becoming victims of ransomware attacks.

As mentioned with the SonicWall incident, the best way to avoid an end of life vulnerability is to update your unpatched software to a more recent version. If the product being supported is no longer being supported altogether, the best course of action is to switch to an alternative that is being supported. In this case, PHP, OpenSSL, and Apache are all still supported. Therefore, in order to remedy this vulnerability, we need only download the latest versions of these softwares and perform the updates.

References

Lakshmanan, R. (2021, July 15). *Ransomware attacks targeting unpatched EOL SonicWall SMA 100 VPN appliances*. The Hacker News. Retrieved February 13, 2022, from https://thehackernews.com/2021/07/ransomware-attacks-targeting-unpatched.html

Security Boulevard. (2020, September 2). *Top Five most infamous ddos attacks*. Security Boulevard. Retrieved February 13, 2022, from https://securityboulevard.com/2020/09/top-five-most-infamous-ddos-attacks/