ROBO6K

# CYBER WRAP-UP

## IN THIS ISSUE

## CONTINUED

A sneaky privilege escalation technique allows a message to bypass windows security. Named NoFilter allows attackers to abuse the Windows Filtering Platform to escalate privileges.

Ivanti systems are affected by a pre-authorization buffer overflow attack. This is concerning as the memory overload can cause systems to crash or arbitrary code to be executed. Due to the nature of the flaw and the impact it could have, it was given a 9.8 severity.

## THIS WEEK

Researchers develop a new and powerful cache poisoning attack named MaginotDNS which has the ability to target TLD.

Microsoft fixes Kernal flaw disclosed to them by Google Project Zero. The flaw was originally turned off as it was thought to introduce breaking changes to Windows.

A critical code injection flaw allows 2,000 Citrix NetScaler instances to become hacked. At least 20 different countries were affected by the backdoor hack resulting in the equipment being weaponized in this large-scale attack.

A new exploit of the Apple iOS 16 allows attackers to trick users into a fake “airplane mode” while using a stealthy cellular data connection to infiltrate the device. This allows attackers to deliver a malicious payload without being detected.

## TAKEAWAYS

While systems being exploited and vulnerabilities are not a new thing, this week continues to point out the need for a robust patch management system. While there is no way to protect every system 100% of the time, it is crucial to keep patching and ensuring that you take every precaution that you can. That being said, it is also of paramount importance to continue to educate end users. While you can patch the servers, network infrastructure and vital components, an unpatched personal device can make the entire system fall apart. Remember, an attacker just needs a small window, and it is up to you to keep it shut as tight as possible.

Social engineering bypasses all technologies, including firewalls.

*Kevin Mitnick*

Research comes from multiple sources. For a deeper dive into the stories found here, you can visit these fantastic sources of information:

https://thehackernews.com/

https://www.bleepingcomputer.com/

**Caleb Leggett**
Account Support

T: 512-501-1223 |
cleggett@robo.net - www.robo.net
2600 S. 1st St, Suite 100.
Austin, TX, 78704