

Week of

12/4-8

As we head into the holiday season, it is important to remember the need for staying on top of your online security. While the need to continuously patch your devices and software is present throughout the year, ensuring that patches are applied and that you maintain good password hygiene is extremely important, both in the professional world but also in your personal life.


Taking a look at some of the notable releases, we will notice that threat actors are working hard to compromise everything from mobile devices to exchange accounts and even federal agency servers. Understanding the attack vectors and how attackers can pivot between them can help to ensure that you can protect against them as best as possible.

First, let's take a look at the release of [android updates](#) to fix a critical RCE flaw. Released as a zero-day, the RCE flaw is concerning as user interaction is not needed to execute and it does not require any additional privileges. As of the writing, Google has not released if the attack has been performed in the wild.

Knowing the systems impacted by vulnerabilities can help to evaluate the risk these may have. The release of [CVE-2023-45866](#) shows that underlying systems, like Bluetooth can cause impact to multiple operating systems. While the fact that the attacker needs to be in close proximity to the target device is of some relief, knowing that they are able to inject keystrokes without user consent.

Knowing that just because a patch has been applied, attackers do not stop and are sometimes able to bypass those helps to highlight the need to keep up with patching. With Microsoft releasing a report that [Russian backed attackers](#) are actively doing this to take over Outlook accounts on their Exchange. Although there is a patch for both the vulnerability and the bypass, there are also additional steps that are needed to fully protect against this attack type bringing to light that just applying the patches is sometimes not enough to fully protect against certain attack types.

This brings us to the brazen attack against [Federal Agency servers](#). Using an improper Access control, an unknown threat group was able to gain initial by exploiting the



Adobe ColdFusion vulnerability. While evidence suggests that this attack was focused more on reconnaissance, this may be only the first portion of the attack. Using HTTP POST commands, the attackers were able to enumerate the directory path that is associated with ColdFusion. While traversing the directory, they also left artifacts within the web server. Additionally, they were able to view the data within the ColdFusion seed.properties file which includes the encryption method used to encrypt passwords.

Looking through these is only the tip of the iceberg within the world. As we wrap up for the week, knowing the importance of staying up to date can never be stressed enough. There are many avenues to do this and even if you are not striving to work within cybersecurity or even technology in general, knowing what is going on will help within your professional life as well as your personal life.

Thank you,

Caleb Leggett

