

Memorandum For: Alejandro Mayorkas

From: Afoma Muojekwu

Subject: Zero-Day Attacks

Main Point:

A new vulnerability has been found in VMware by attackers, and without proper mitigation could lead to the leak of sensitive information through the use of many more software virtualization appliances. Therefore, a recommendation would be to emphasize the importance of being able to identify zero-day attacks as they occur to the CISA, as well as having a plan set in place to mitigate it prior.

Background:

The vulnerability is CVE-2023-34048 which is an out of bounds write that an attacker can use to do remote code execution. The malware families involved were VIRTUALPITA and VIRTUALPIE to target the virtual machines managed by VMware. This makes way for more of VMware's vulnerabilities to run commands and make file transfers to and from guests and hosts. The group that has struck VMware is known for targeting these zero-day vulnerabilities, meaning that there may very well be more on the way.

Options:

Option 1: Warn those in charge of how to go about zero-day attacks as they are in motion. This could be done with a defense approach that implements patch management and proper training.

Option 2: Prepare a risk assessment for all vulnerabilities.

Option 3: Observe the weakest links in the system, note them, and make use of IDPS, firewalls, and encryption of data.

Conclusion:

It is near impossible to predict every single zero-day attack that may occur before an occurrence, so I recommend training that helps combat these zero-day attacks as they happen, should they happen. Have plans set in place to validate the attack and collect additional data that may be needed. I'd also recommend being prepared by knowing the vulnerabilities in the system beforehand and prioritizing the ones that are the most high risk, so you know what to keep an eye on as the weakest link with the most to offer is likely to be targeted.