



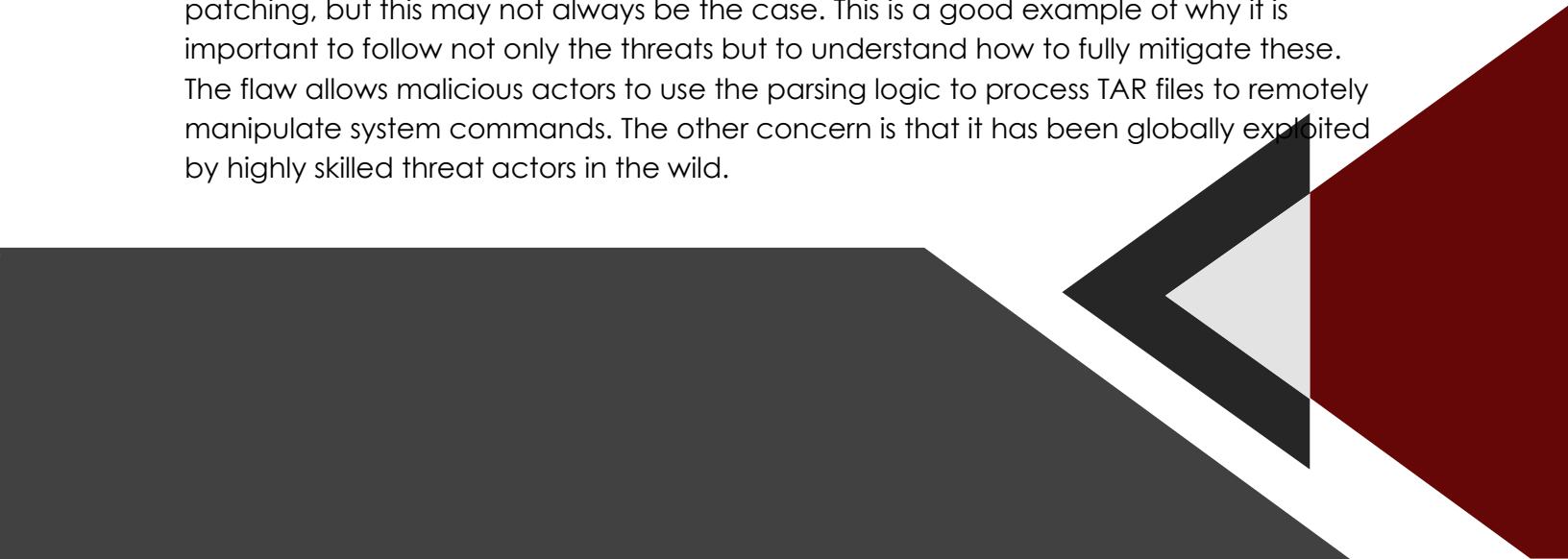
Top vulnerabilities of 2023

It's that time again to take a brief look into the world of Cyber Security. For this installment, I would like to take a look back at this year's top vulnerabilities. While it is important to keep up with every week, it is also important to take a look at the year as well. Let's jump right into it. These are based on the [Qualys survey](#) and more information can be found in this link. Unfortunately, the severity and business impact can vary from company to company depending on the exposure which is why it is important to understand your attack surface.

Starting with #10, [the SugarCRM](#) ranks in with an 8.8 CVSS score. The flaw is suspected of being exploited by a single threat actor in the wild. The vulnerability allows threat actors to inject PHP code into the CRM platform module and allows for authentication bypass and remote code execution. Unfortunately, the current patch rate is at 36% which signifies a massive number of vulnerable systems in the wild.

Next up is the [VMware Aria Operations](#) command injection vulnerability. As this is a key system in orchestrating network infrastructure which results in a CVSS score of 9.8. This brings to light the need to stay up with network security as this is the backbone of the organization. The vulnerability allows threat actors to inject code with administrative privileges and could result in the compromise of a considerable part of the network.

Coming in at #8, the [Barracuda email security gateway](#) flaw holds a CVSS score of 9.8 and while a patch has been released we see the rare recommendation from Barracuda to completely replace the affected hardware to prevent a persistent backdoor access. This is important to note as many vulnerabilities can be fixed with patching, but this may not always be the case. This is a good example of why it is important to follow not only the threats but to understand how to fully mitigate these. The flaw allows malicious actors to use the parsing logic to process TAR files to remotely manipulate system commands. The other concern is that it has been globally exploited by highly skilled threat actors in the wild.




While the next vulnerability holds only a CVSS score of 7.8, the outcome of the attack gives the threat actors access to create a gateway with root level access. Known as the Windows common log file system driver vulnerability, the escalation of privileges on the Windows 2003 R2 server can allow threat actors to inject malware and weaponize the flaw to distribute ransomware. This attack affects the pivotal logging subsystem and can have dire consequences if not properly patched.

Coming in at # 6 is the supply chain attack of the 3CX VoIP system. By trojanizing the desktop client, attackers can siphon off system data and extract credentials from stored browsers on both Windows and macOS present a huge risk. With a CVSS score of 7.8, the average gestation of this attack is 78 days which means that it takes longer to identify the intrusion. However, a fast 7-day remediation suggests that once the flaw is discovered, it can be fixed relatively quickly.

As we hit the halfway point, the #5 attack of the MoveIT transfer injection comes in with a CVSS score of 9.8 and while patching was applied, the vulnerability is still prevalent as backups are moved into production without the correct QC on patches applied to the backups before being moved into production. Prevalent ransomware gangs have been able to extract significant amounts of data by using the SQL injection flaw and with only 51% of systems fully patched, the flaw still holds considerable risks to organizations.

Next up, let's look at the Microsoft Outlook elevation of privileges vulnerability. This is significant as the flaw is initiated by an incoming email and the payload is deployed as soon as the Outlook server processes it. This allows for the threat to bypass many preventative measures. With an average breach age of 89 days, attackers have ample time to gain access to privileged information and affect the confidentiality of the data. Holding a CVSS score of 9.8, this threat represents a significant threat. On the bright side, there has been roughly 87.5% of systems that have already been patched to mitigate this threat.

As we get closer to the top ranked vulnerability, it is important to remember that knowing your attack surface and what systems you need to patch or replace is of paramount importance. Hitting the #3 spot, the Fortra GoAnywhere RCE flaw allows attackers to gain access to the managed file transfer system and inject code. The risk



can result in complete takeover of the MFT server and allows attackers to inject ransomware, steal confidential information and pivot into other internal networks systems. With only 33% of systems patched, this still represents a substantial risk to organizations.

We are inching closer to our top spot! Although the #2 spot holds a CVSS score of only 4.4, it is strongly recommended that you do not overlook the [Windows smart screen security bypass vulnerability](#). The main reason for falling in such a high position is that it allows attackers to bypass security mechanisms, specifically the Mark of The Web defenses which is an important part of SmartScreen. This makes it much easier for threat actors to spread malicious payloads without detection.

Finally, the #1 spot for the year so far is the [PaperCut NG/MF Multiple security vulnerabilities](#). Coming with a severity of 9.8, the vulnerability raises a huge risk as it can lead to entire network takeover. Allowing threat actors to inject ransomware due to inadequate access control, they are able to inject code with elevated privileges. An average patch rate of only 59% leads to many vulnerable systems still in the wild. Attackers have an average intrusion time of 97 days which gives ample time to perform the code injection and do what they want before detection.

Since we have not fully completed the year, this list may change some and of course is based on the perspective of one company so again I stress the importance of keeping up with all CVE announcements and the trending news within the world of cyber security. Remember that you as the technical specialist are the protection for the people that you protect.

Caleb Leggett

