



By: Caleb Leggett

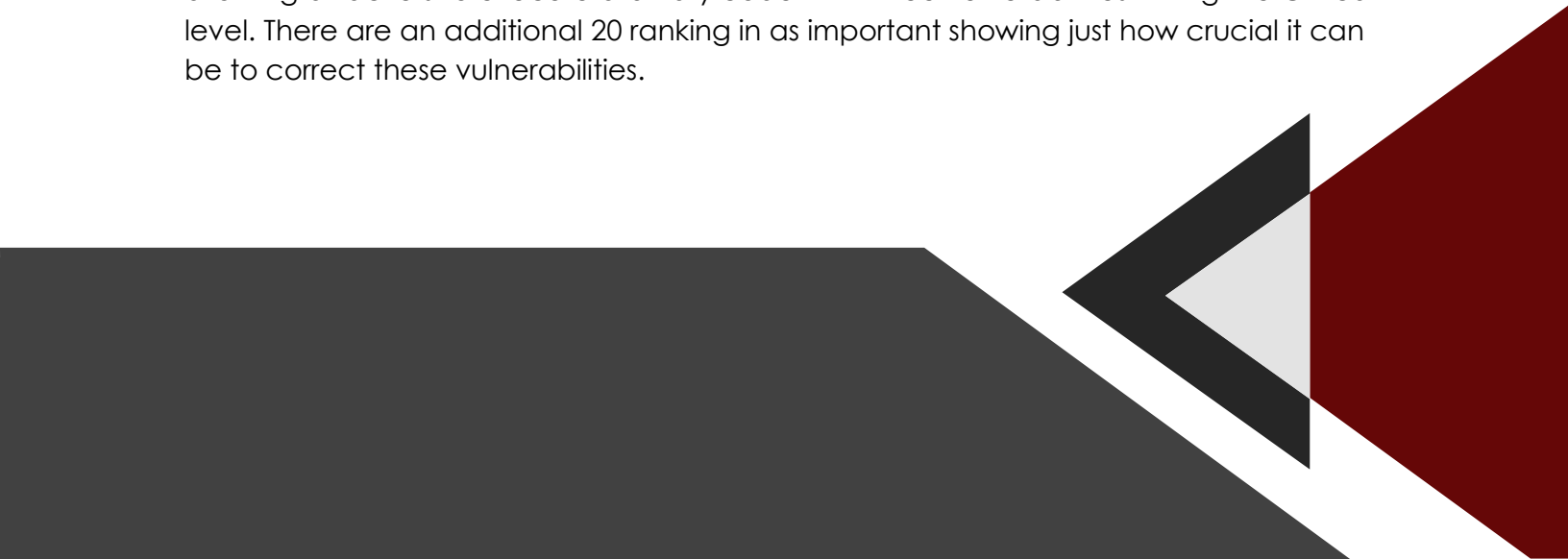
September Windows Patch Recap


As many in the security industry know, system patching can become an extremely crucial part to keep up with as you work to create the best security posture that you can. Knowing exactly what you are fighting against can help in the decision-making process on if and when patches are pushed to the endpoints you have been charged with protecting. Join me on the journey through the latest September patches that were released from Microsoft to help give you insight into why it is important to stay up with these.

Looking at the high level, a total of 79 flaws were corrected in the patch Tuesday release. These include a wide range of vulnerabilities including actively exploited vulnerabilities as well as a publicly disclosed Zero-Day. Ensuring to highlight the fact that this is a high number of flaws, these types of numbers are not uncommon. This should help to guide you in the decision-making process.

As we dive one layer deeper, we will look at the range of flaws that were patched this month. These flaws include a wide range of attack vectors, some may become more detrimental than others which can drive the decisions on the criticality of deployment. Starting with the lower impact flaws, we see 3 Spoofing, 8 Denial of Service and 11 Information disclosure vulnerabilities. While these may represent a lower risk of impact, that does not make them less important to correct.

Taking a look at the next three categories, these may represent a higher impact risk to an organization if they are exploited. Starting with the Remote Code Execution, allowing attackers to execute arbitrary code with three vulnerabilities hitting the Critical level. There are an additional 20 ranking in as important showing just how crucial it can be to correct these vulnerabilities.





Next up on the higher risk vulnerabilities include a total of 4 Security Feature Bypass vulnerabilities. These of course will rank higher risk as they allow attackers to get around the systems and features that are meant to protect the endpoint. As a defender, it is important to safeguard the tools and features that provide the protection of the systems maintain the integrity to provide continuous protections.

Finally, with the highest numbers we look at the Privilege Escalation Vulnerabilities. By using this attack vector, the threat actors can gain elevated privileges. This ensures that they can carry out attacks that may require these elevated privileges without taking over another account. In the release, Microsoft addresses a total of 30 of these types of flaws.

Of course, we have focused only on the Microsoft patches, but I hope that this shows the importance of keeping up with the releases from the software that you as the admin support.

Resources:

[September Patch Tuesday](#)

