20 MOST EXPLOITED VULNERABILITIES IN 2021

vFeed.io

The number of vulnerabilities in 2021 have dramatically increased so that the technical teams in charge of the patch management find themselves drowning in a myriad of critical and urgent tasks.

Because in a perfect world, the organizations must be aware when a vulnerabilities are released, especially the critical ones. That's why the vulnerability management process can rapidly turn into a nightmare challenge when the companies are managing thousands of assets.

However, a few stood out from the crowd, so let me introduce the **2021 Top Vulnerabilities** as well as the indicators generated by our vulnerability intelligence service in order to provide your organizations with a transverse approach to identify, scan, detect, block, fix and even exploit your resources.

In this review, we have extended the list to the **Top Twenty Severe Security Vulnerabilities for year 2021**.

You should immediately take whatever steps, if not done yet, you can to reduce the threat to you. In most cases, the responsible party has already released a fix.

TOP 20 EXPLOITED VULNERABILITIES

Based on vFeed Indicators of Vulnerability (IoVs)

- Number proof-of-concepts per vulnerability
- Ease of Exploitability
- High Popularity Ratio
- Weaponization of the exploit
- Malware based campaigns

1. **CVE-2021-44228** : Apache Log4j Remote Code Execution Vulnerability (*codename:* ***Log4Shell***)
2. **CVE-2021-4034** : Linux Polkit's “pkexec” utility Local Privilege Escalation Vulnerability (*codename:* ***PwnKit***)
3. **CVE-2021-41773 :** Apache HTTP Server Path Traversal & Remote Code Execution.
4. **CVE-2021-3156**: Sudo Heap-Based Buffer Overflow Vulnerability (*codename:* ***Baron Samedit***)
5. **CVE-2021-26855**: Microsoft Exchange Server Remote Code Execution Vulnerability (*codename:* ***ProxyLogon***)
6. **CVE-2021-26084**: Confluence Server OGNL Injection
7. **CVE-2021-1675**: Windows Print Spooler Remote Code Execution Vulnerability (*codename:* ***PrintNightmare***)
8. **CVE-2021-40444**: Microsoft MSHTML Remote Code Execution Vulnerability.
9. **CVE-2021-21972**: VMware vCenter Server Remote Code Execution Vulnerability.
10. **CVE-2021-43798**: Grafana Path Traversal Vulnerability

11. **CVE-2021-22205** : GitLab Unauthenticated Remote Code Execution Vulnerability
12. **CVE-2021-42013**: Apache HTTP Server Insecure Path Normalization Vulnerability
13. **CVE-2021-36934:** Windows Elevation of Privilege Vulnerability (*codename:* ***HiveNightmare / SeriousSam***)
14. **CVE-2021-3560**: Linux Polkit Package Privilege Escalation.
15. **CVE-2021-22204**: ExifTool Arbitrary Code Execution.
16. **CVE-2021-22986**: F5 BIG-IP Remote Code Execution Vulnerability.
17. **CVE-2021-21300**: Git for Visual Studio Remote Code Execution Vulnerability.
18. **CVE-2021-38647**: Microsoft Azure Open Management Infrastructure Remote Code Execution (*codename:* ***OmiGod***).
19. **CVE-2021-22005**: VMware vCenter Analytics Service Arbitrary File Upload Vulnerability.
20. **CVE-2021-21985**: VMware vCenter Server Remote Code Execution Vulnerability.

TOP 20 EXPLOITED VULNERABILITIES

Based on vFeed Indicators of Vulnerability (IoVs)

- Number proof-of-concepts per vulnerability
- Ease of Exploitability
- High Popularity Ratio
- Weaponization of the exploit
- Malware based campaigns

CONCLUSION

We have observed a very quick execution in the process of **exploits weaponization**. Indeed, when a vulnerability is revealed, a range of exploits are immediately released in the wild.
That's may be a result of the **bug bounty** phenomenon and the excessive competitiveness between the different participants.

The most relevant exploits are therefore **automated** and can be easily reused in mass attacks or even leveraged in the design of a malware chain attack. This obviously complicates the life of security operations, & administrators during the deployment of patches & fixes.

Which brings us to the unequivocal observation: SecOps and other security experts must certainly integrate **vulnerability intelligence** methods into their strategy which will make it possible to identify the warning signs (weak signals) of an imminent targeted attack.

*The **Indicators of Vulnerability IoVs** for the **Top Twenty Severe Security Vulnerabilities for year 2021** can be obtained from support@vfeed.io*