Top 30 serious security holes are being exploited by hackers the most

Recently, the cybersecurity agencies of Australia, the UK and the US have issued a joint report detailing the most exploited vulnerabilities in 2020 and 2021.

This report shows that cybercriminals can quickly turn a publicly reported vulnerability into a weapon to their advantage.

This report also includes a list of the top 30 critical security holes that are being exploited by hackers the most. These 30 vulnerabilities appear in a variety of software including teleworking, virtual private networks (VPNs), and cloud-based technologies. These are products of many big names such as Microsoft, VMware, Pulse Secure, Fortinet, Accelion, Citrix, F5 Big IP, Atlassian and Drupal.

Here are the most exploited critical security holes in 2020:

1. CVE-2019-19781 (CVSS score: 9.8): Citrix Application Delivery Controller (ADC) and Gateway Directory Transport Vulnerability
2. CVE-2019-11510 (CVSS score: 10.0): Pulse Connect Secure arbitrary file reading vulnerability
3. CVE-2018-13379 (CVSS score: 9.8): Fortine FortiOS pipeline vulnerability leads to system file leak
4. CVE-2020-5902 (CVSS score: 9.8): F5 BIG-IP Remote Code Execution Vulnerability
5. CVE-2020-15505 (CVSS score: 9.8): MobileIron Core & Connector Remote Code Execution Vulnerability
6. CVE-2020-0688 (CVSS score: 8.8): Microsoft Exchange memory corruption vulnerability
7. CVE-2019-3396 (CVSS score: 9.8) - Atlassian Confluence Server remote code execution vulnerability
8. CVE-2017-11882 (CVSS score: 7.8) - Microsoft Office memory corruption vulnerability

9. CVE-2019-11580 (CVSS score: 9.8) - Atlassian Crowd and Crowd Data Center remote code execution vulnerability
10. CVE-2018-7600 (CVSS score: 9.8) - Drupal Remote Code Execution Vulnerability
11. CVE-2019-18935 (CVSS score: 9.8) - Telerik .NET decryption vulnerability leads to remote code execution
12. CVE-2019-0604 (CVSS score: 9.8) - Microsoft SharePoint Remote Code Execution Vulnerability
13. CVE-2020-0787 (CVSS score: 7.8) - Windows Platform Intelligent Transport Service (BITS) privilege escalation vulnerability
14. CVE-2020-1472 (CVSS score: 10.0) - Windows Netlogon Privilege Escalation Vulnerability

List of the most actively exploited security vulnerabilities so far in 2021:

1. Microsoft Exchange Server: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 (also known as "ProxyLogon")
2. Pulse Secure: CVE-2021-22893, CVE-2021-22894, CVE-2021-22899 and CVE-2021-22900
3. Accelion: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104
4. VMware: CVE-2021-21985
5. Fortinet: CVE-2018-13379, CVE-2020-12812 and CVE-2019-5591

According to experts, cybercriminals are increasingly exploiting software vulnerabilities to attack large groups of objects, including both private and institutional, around the world. However, users and organizations can mitigate the damage of these reported vulnerabilities by updating patches early and implementing a centralized patch management system.