2020 MOST EXPLOITED *VULNERABILITIES*

Correlated by

vFeed.io

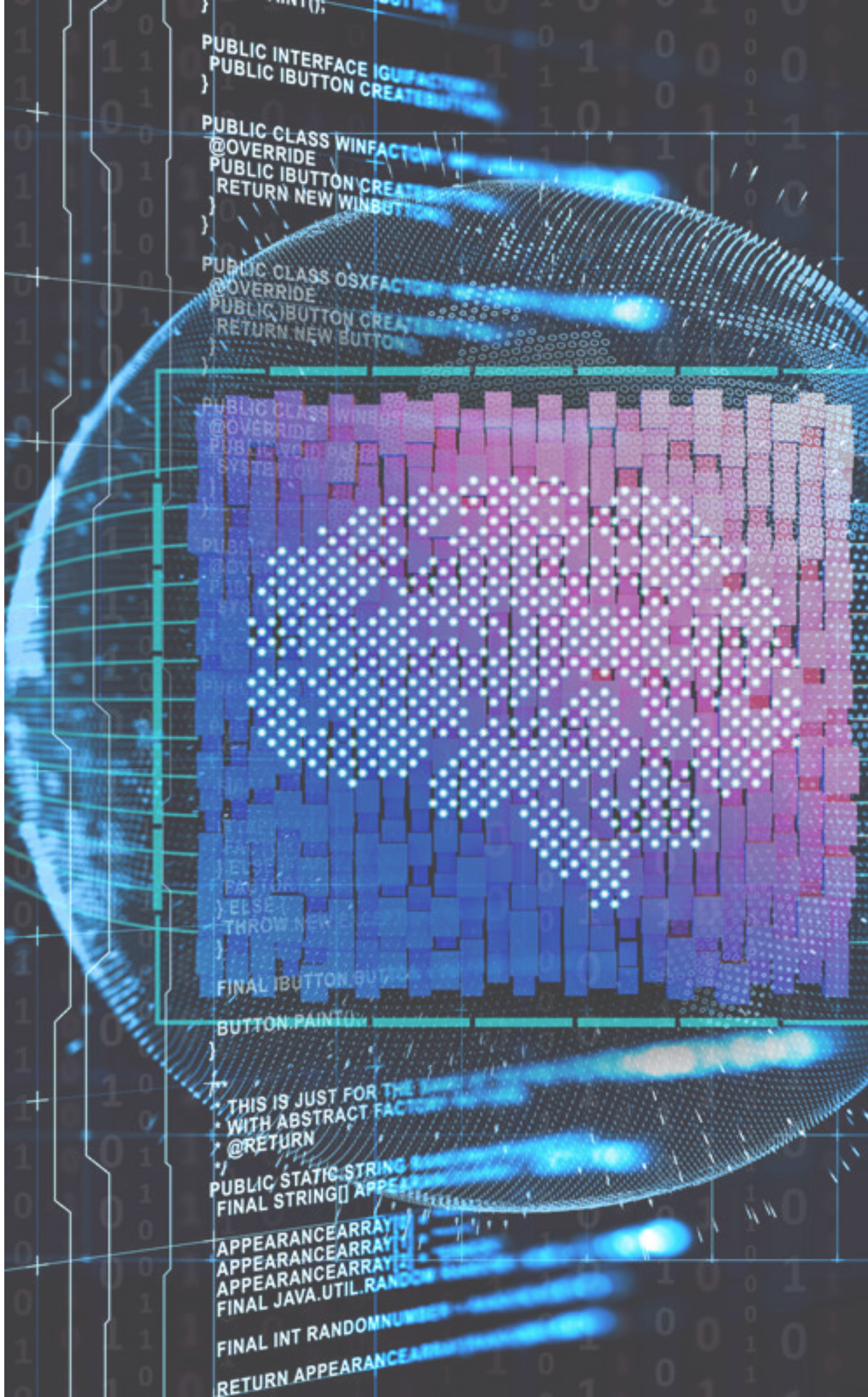
TIME TO FIX SOME ...

Every day, new common vulnerabilities and exploits are publicly exposed. While this brings these flaws to the public's attention and allows users to patch them, it also alerts potential attackers to their existence.

We went and dive into the tons of vulnerability intelligence data we accumulated over the years. I love to see patterns as I firmly believe that there will be always someone out there that will give these data a meaning !!

In this review, you'll find the list of the **Top Ten Severe Security Vulnerabilities for year 2020**.

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 10 EXPLOITED VULNERABILITIES

Based on Vulnerability Indicators

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

1. **CVE-2020-0796** : Windows SMBv3 Client/Server Remote Code Execution Vulnerability (*codename:* ***SMBGhost***)
2. **CVE-2020-5902**: F5 Networks BIG-IP TMUI RCE vulnerability
3. **CVE-2020-1472:** Microsoft Netlogon Elevation of Privilege (*codename:* ***Zerologon***)
4. **CVE-2020-0601**: Windows CryptoAPI Spoofing Vulnerability (*codename:* ***CurveBall***)
5. **CVE-2020-14882**: Oracle WebLogic Server RCE
6. **CVE-2020-1938**: Apache Tomcat AJP File Read/Inclusion Vulnerability (*codename:* ***GhostCat***)
7. **CVE-2020-3452**: Cisco ASA and Firepower Path Traversal Vulnerability
8. **CVE-2020-0688**: Microsoft Exchange Server Static Key Flaw Could Lead to Remote Code Execution
9. **CVE-2020-16898**: Windows TCP/IP Vulnerability (*codename:* ***Bad Neighbor)***
10. **CVE-2020-11651**: SaltStack RCE Authentication Bypass
    CVE-2020-1350: Critical Windows DNS Server RCE. (*codename:* ***SIGRed)***