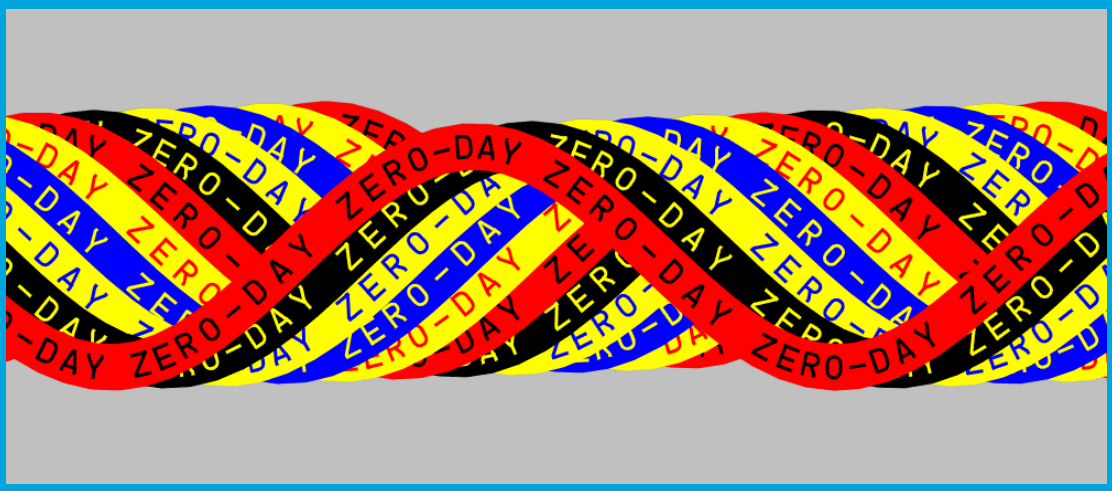
Security Newsletter

8 February 2021

Subscribe to this newsletter

Proper patching would have prevented 25% of all zero-days found in 2020



Google said today that a quarter of all the zero-day vulnerabilities discovered being exploited in the wild in 2020 could have been avoided if vendors had patched their products correctly. The company, through its Project Zero security team, said it detected 24 zero-days exploited by attackers in 2020. Six of these were variations of vulnerabilities disclosed in previous years, where attackers had access to older bug reports so they could study the previous issue and deploy a new exploit version.

This situation could have been avoided if vendors had investigated the root cause of the bugs in greater depth and invested more into the patching process. Zero-days provide a window into an attacker's mind that defenders should take advantage of and try to learn about the entry vectors an attacker is trying to exploit, determine the vulnerability class, and then deploy comprehensive mitigations.

Being able to correctly and comprehensively patch isn't just flicking a switch: it requires investment, prioritization, and planning. It also requires developing a patching process that balances both protecting users quickly and ensuring it is comprehensive, which can at times be in tension. While we expect that none of this will come as a surprise to security teams in an organization, this analysis is a good reminder that there is still more work to be done.

Read More on ZDNet

Even More on Google Project Zero blog

Account takeover attacks spiked in 2020

Kaspersky has released the results of research into fraud detected by its Fraud Prevention platform in 2020, and the results further reinforce what we already knew: 2020 was a banner year for online fraudsters, with account takeovers dominating as the method of choice. Occurring whenever a bad actor is able to steal login credentials and seize control of an online account, takeover attacks rose from 34% of fraud detected by Kaspersky in 2019 to 54% by the end of December 2020.

Other methods of fraud were blips on the radar compared to account takeovers: The next most popular method, at just 16% of detected fraud, was money laundering/mule transactions, followed by new account fraud (14%), and a mere 12% of instances used remote access or hacking tools to accomplish their goals. In short, when it comes to fraud, account takeovers should be the No. 1 concern for individuals and businesses heading into 2021, especially as social distancing and remote work continue to be the norm.

Kaspersky makes several recommendations all online services and retailers should adopt to help stem the tide of account takeovers: Limit the number of times a transaction, such as logging in, can be attempted. Send out regular emails to customers warning them of the latest fraud trend. Annual security audits, along with penetration tests, should become standard practice. Have a team dedicated to fraud analysis that can keep up on trends and analyze attacks to find solutions. Implement multifactor authentication on all accounts.

Read More on TechRepublic

Even More on Kaspersky Blog

More #News

- Plex Media servers are being abused for DDoS attacks

- Malware Targets Kubernetes Clusters
- Hacking group also used an IE zero-day against security researchers
- Google Vulnerability Reward Program: 2020 Year in Review
- New Matryosh DDoS Botnet Targeting Android-Based Devices
- Android devices ensnared in DDoS botnet
- Latest macOS Big Sur also has SUDO root privilege escalation flaw
- Malicious script steals credit card info stolen by other hackers
- Security chaos engineering helps you find weak links in your cyber defenses before attackers do
- Ransomware: Average Ransom Payment Declines to $154,108 as Gangs Fail to Honor Data Deletion Promises
- A New Software Supply–Chain Attack Targeted Millions With Spyware

#Breach Log

- Security firm Stormshield discloses data breach, theft of source code
- Trucking Giant 'Forward Air' Says Ransomware Attack Had $7.5M Impact
- Oxfam Australia investigates data breach after database sold online
- Female escort review site data breach affects 470,000 members
- US federal payroll agency hacked using SolarWinds software flaw
- Data breach exposes 1.6 million Washington unemployment claims
- Exposed Azure bucket leaked passports, IDs of volleyball reporters

#Patch Time!

- New Chrome Browser 0-day Under Active Attack
- Critical Flaws Reported in Cisco VPN Routers for Businesses
- Critical Bugs Found in Popular Realtek Wi-Fi Module for Embedded Devices
- Siemens Releases Patches to Prevent Remote Takeover of SIMATIC HMI Panels
- SonicWall fixes actively exploited SMA 100 zero-day vulnerability
- Cisco fixes critical code execution bugs in SMB VPN routers
- Weak ACLs in Adobe ColdFusion Allow Privilege Escalation
- SolarWinds patches critical vulnerabilities in the Orion platform
- Libgcrypt developers release urgent update to tackle severe vulnerability

#Tech and #Tools

- A tale of EDR bypass methods
- Renew Azure Key Vault Certificates from Let's Encrypt
- PatrowlHears — Open-Source Vulnerability Intelligence Center
- Crown Jewels Analysis: Identify your most critical cyber assets
- Seven Common Microsoft Active Directory Misconfigurations that Adversaries Abuse
- Detecting Secrets to Reduce Attack Surface
- Abusing Google Chrome extension syncing for data exfiltration and C&C
- Objective-See projects, now all Open-Source

- The Kerberos Credential Thievery Compendium (GNU/Linux)
- A framework for effective corporate communication after cyber security incidents
- Microsoft azure ad conditional access validator
- ScareCrow: Payload generator to bypass EDR
- Google funds project to secure Apache web server with new Rust component

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us