

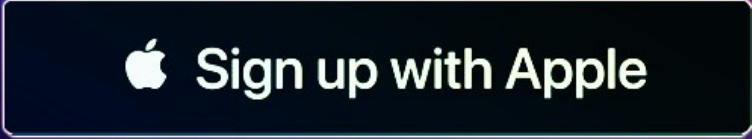



Security Newsletter

8 June 2020

[Subscribe to this newsletter](#)

Critical 'Sign in with Apple' Bug Could Have Let Attackers Hijack Anyone's Account



 Sign up with Apple

Into Anyone's Account

Apple recently paid Indian vulnerability researcher Bhavuk Jain a huge \$100,000 bug bounty for reporting a highly critical vulnerability affecting its 'Sign in with Apple' system. The now-patched vulnerability could have allowed remote attackers to bypass authentication and take over targeted users' accounts on third-party services and apps that have been registered using 'Sign in with Apple' option.

Launched last year at Apple's WWDC conference, 'Sign in with Apple' feature was introduced to the world as a privacy-preserving login mechanism that allows users to sign up an account with 3rd-party apps without disclosing their actual email addresses (also used as Apple IDs). "The impact of this vulnerability was quite critical as it could have allowed a full account takeover. Many developers have integrated Sign in with Apple since it is mandatory for applications that support other social logins. To name a few that use Sign in with Apple - Dropbox, Spotify, Airbnb, Giphy (now acquired by Facebook)," Bhavuk added.

The researcher responsibly reported the issue to the Apple security team last month, and the company has now patched the vulnerability. Besides paying bug bounty to the researcher, in response, the company also confirmed that it did an investigation of their server logs and found the flaw was not exploited to compromise any account.

[Read More on TheHackerNews](#)

[Even More on WeLiveSecurity](#)

48% of employees are less likely to follow safe data practices when working from home



In a survey of 1,000 people from the US and 1,000 from the UK, Tessian researchers found that 48% are less likely to follow safe data practices when working from home and 84% of IT leaders surveyed said data loss prevention is more challenging when employees are working from home.

When asked why they put their company and its data at risk, employees gave a variety of answers, with half saying "not being watched by IT" was their main reason for not following safe data practices. Another 47% said distractions at home caused them to take more chances and 51% say security policies impeded their productivity while 40% cited the pressure to get work done quickly as a reason. Of those surveyed, 54% said they would find workarounds if security policies stop them from doing their jobs.

A recent report on data breaches from Verizon found that 30% of breaches involve internal actors exposing company information as a result of negligent or malicious acts and the Tessian study confirms many of Verizon's findings.

[Read More on TechRepublic](#)

More #News

- [New Tycoon ransomware targets both Windows and Linux systems<](#)
- [Any Indian DigiLocker Account Could've Been Accessed Without Password](#)
- [Fitness Depot hit by data breach after ISP fails to 'activate the antivirus'](#)
- [uBlock Origin ad blocker now blocks port scans on most sites](#)
- [Critical Vulnerability Could Have Allowed Hackers to Disrupt Traffic Lights](#)
- [Bruteforce malware probes login for popular web platforms](#)
- [Here are the new security features in Windows 10 2004](#)
- [Phishers Use Fake VPN Alerts to Steal Office 365 Passwords](#)
- [Hackers tried to steal database logins from 1.3M WordPress sites](#)
- [Big GDPR Fines in UK and Ireland: What's the Holdup?](#)
- [\(Bad\) Password Changing Habits After a Breach](#)

#Patch Time!

- [Thousands of Exim Servers Vulnerable to Critical Flaw: Report](#)
- [Cisco Patches Dozen Vulnerabilities in Industrial Routers](#)
- [Grafana 6.7.4 and 7.0.2 released with important security fix](#)
- [Mozilla fixes five high-risk Firefox flaws, bug in DoH feature](#)
- [Newly Patched SAP ASE Flaws Could Let Attackers Hack Database Servers](#)
- [Critical VMware Cloud Director Flaw Lets Hackers Take Over Corporate Servers](#)

#Tech and #Tools

- [Active Directory Security Assessment Checklist](#)
- [APICheck - The DevSecOps toolset for HTTP APIs](#)
- [Apache Tomcat RCE by deserialization \(CVE-2020-9484\) – write-up and exploit](#)
- [Understanding Certificate Pinning/a>](#)
- [Analyzing Honeypot Data with Sentinel](#)
- [Set up an SSH bastion on AWS with Terraform modules in few minutes](#)
- [shodan-dojo: Learning Shodan through katas](#)
- [Zero-day in Sign in with Apple](#)
- [The Octopus Scanner Malware: Attacking the open source supply chain](#)
- [Evolution of Excel 4.0 Macro Weaponization](#)
- [nuclei: configurable targeted security scanner based on templates](#)
- [The Elastic Guide to Threat Hunting](#)
- [Covenant v0.5 released](#)
- [Evading WinDefender ATP credential-theft: kernel version](#)

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>