kindred

Security Newsletter

2 December 2019

Subscribe to this newsletter

Magento Marketplace Suffers Data Breach Exposing Users' Account Info

If you have ever registered an account with the official Magento marketplace to bought or sold any extension, plugin, or e-commerce website theme, you must change your password immediately.

Adobe—the company owning Magento e-commerce platform—today disclosed a new data breach incident that exposed account information of Magento marketplace users to an unknown group of hackers or individuals. According to the company, the hacker exploited an undisclosed vulnerability in its marketplace website that allowed him to gain unauthorized third-party access to the database of registered users — both customers (buyers) as well as the developers (sellers). The leaked database includes affected users' names, email addresses, MageID, billing and shipping address information, and some limited commercial information.

Though Adobe hasn't explicitly mentioned that the account passwords were also leaked, users are still recommended to change it, and do the same for any other website where you are using the same password.

Read More on TheHackerNews

Even More on BankInfoSecurity

Dozens of Severe Flaws Found in 4 Popular Open Source VNC Software

Four popular open-source VNC remote desktop applications have been found vulnerable to a total of 37 security vulnerabilities, many of which went unnoticed for the last 20 years and most severe could allow remote attackers to compromise a targeted system.

There are numerous VNC applications, both free and commercial, compatible with widely used operating systems like Linux, macOS, Windows, and Android. Considering that there are currently over 600,000 VNC servers accessible remotely over the Internet and nearly 32% of which are connected to industrial automation systems, cybersecurity researchers at Kaspersky audited four widely used open source implementation of VNC, including LibVNC, UltraVNC, TightVNC and TurboVNC.

But, exploiting this flaw requires authentication credentials to connect to the VNC server or control over the client before the connection is established. Therefore, as a safeguard against attacks exploiting server-side vulnerabilities, clients are recommended not to connect to untrusted or untested VNC servers, and administrators are required to protect their VNC servers with a unique, strong password. Kaspersky reported the vulnerabilities to the affected developers, all of which have issued patches for their supported products, except TightVNC 1.x that is no longer supported by its creators. So, users are recommended to switch to version 2.x.

Read More on TheHackerNews

A decade of hacking: The most notable cyber-security events of the 2010s

The 2010s decade is drawing to a close and ZDNet is looking back at the most important cyber-security events that have taken place during the past ten years. Over the past decade, we've seen it all. We've had monstrous data breaches, years of prolific hacktivism, plenty of nation-state cyber-espionage operations, almost non-stop financially-motivated cybercrime, and destructive malware that has rendered systems unusable.

Below is a summary of the most important events of the 2010s, ordered by year. We didn't necessarily look at the biggest breaches or the most extensive hacking operations but instead focused on hacks and techniques that gave birth to a new cyber-security trend or were a paradigm shift in how experts looked at the entire field of cyber-security.

Read More

More #News

- How cyberinsurance works to protect companies in case of a security breach
- OnePlus Suffers New Data Breach Impacting Its Online Store Customers
- New bypass disclosed in Microsoft PatchGuard (KPP)
- Cheap kids smartwatch exposes the location of 5,000+ children
- A hacking group is hijacking Docker systems with exposed API endpoints
- Firefox gets tough on tracking tricks that sneakily sap your privacy
- Ransomware Locks Medical Records at Great Plains Health
- Restaurant Chain: Malware Infected PoS Devices
- Harnessing the Power of the People: Cloudflare's First Security Awareness Month Design Challenge Winners
- Joker's Stash Advertises More Stolen Payment Card Data
- Cryptoqueen: How this woman scammed the world, then vanished
- TrackingTheTrackers: check if a website is disguising third-party trackers as first-party trackers.
- Zero trust architecture design principles
- Malvertising: What It Is and How to Protect Yourself
- Netflix account freeze – don't click, it's a scam!

#Patch Time!

- Splunk customers should update now to dodge Y2K-style bug
- Kaspersky Patches Several Vulnerabilities in Web Protection Features
- HPE warns of impending SSD disk doom
- Dozens of VNC Vulnerabilities Found in Linux, Windows Solutions

#Tech and #Tools

- Jackdaw: Domain information collection & visualisation
- Public SSH keys can leak your private infrastructure
- Troubleshooting with Wireshark: The Case of the TCP Challenge ACK
- Latest Kali Linux OS Added Windows-Style Undercover Theme for Hackers
- Use attribute-based access control with AD FS to simplify IAM permissions management
- Forget homomorphic encryption, here comes functional encryption
- Google Exposed Firebase Database
- Merlin: A cross-platform post-exploitation HTTP/2 Command & Control Tool
- Impersonating JA3 Fingerprints
- JA3Transport Go Library
- AppLocker Internal Part 3 - Access Tokens and Access Checking
- Applocker Internals Part 4 - Blocking DLL Loading

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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