Security Newsletter

14 October 2019

Subscribe to this newsletter

C is for Credit Card: MageCart Hits Volusion E-Commerce Sites

Hackers compromised the infrastructure of Volusion cloud-based e-commerce platform to inject customer checkout pages with malicious JavaScript code that steals payment card data. The attackers added code for dynamic injection of the card data thieving script to a JavaScript that is part of the Volusion e-commerce software. Thousands of websites are likely loading the attackers' script and sending payment information to their server. Some may have been compromised as early as September 12.

Check Point security researcher Marcel Afrahim discovered the compromise while shopping on Sesame Street Live Store, a website from Feld Entertainment that sells official Sesame Street merchandise. The store is built with Volusion, who even provides the nameservers. On the checkout page, Afrahim noticed JavaScript code loading from Google Cloud Storage (storage.googleapis.com), a file storage web service for storing and accessing data on Google Cloud Platform infrastructure. The oddity was that this was the only resource loaded from a source other than 'sesamestreetlivestore.com' or 'volusion.com' affiliated websites.

On the company page, Volusion boasts 30,000 merchants actively using the platform. They are from a variety of fields and the dedicated page shows merchants selling products in the apparel, home and garden, health and beauty, auto and industry, and electronics categories. From our checks, not all of them are still in business. Following reports from news outlets and security researchers, Volusion addressed the issue a few hours ago. Before that, Google took steps and displayed the red 'malware danger' warning when visiting websites loading the malicious JavaScript.

Read More on BleepingComputer

You Gave Your Phone Number to Twitter for Security and Twitter Used it for Ads

Twitter announced that the phone numbers and email addresses of some users provided for two-factor authentication (2FA) protection had been used for targeted advertising purposes—though the company said it was 'unintentional.'

In a blog post, the company said an 'error' in its 'Tailored Audiences and Partner Audiences advertising system' inadvertently used the information provided by users for security reasons to run targeted ads based on the advertisers' own marketing lists. However, Twitter assured that no personal data was ever shared externally with its advertising partners or any other third-parties that used the Tailored Audiences feature.

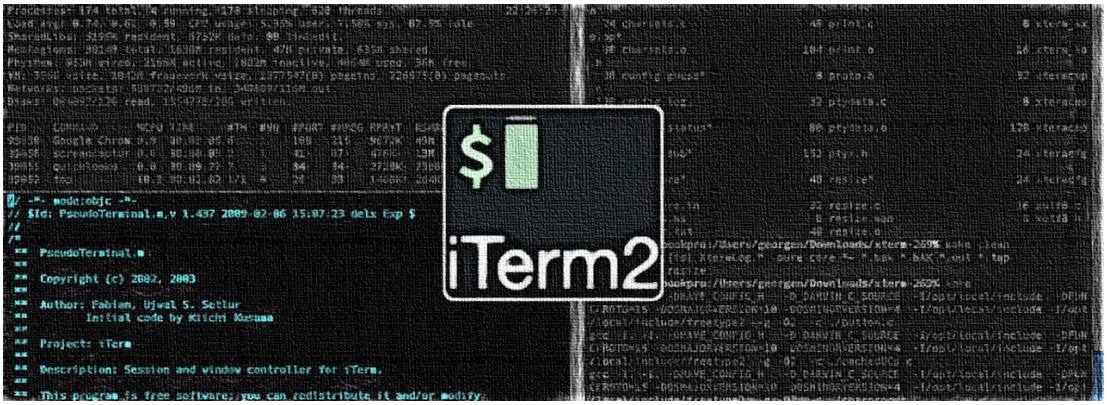
The social networking company also said that it does not know how many users were impacted by this error. Last year, Facebook was also caught using phone numbers provided by its users for 2FA protection; however, in that case, the FTC accused the company of intentionally using that data for advertising purposes—which became one of the reasons FTC issued a $5 billion fine against Facebook in July this year.

The involvement of mobile numbers entered by users to enable security is unfortunate, but we wouldn't advise removing this data in case it proves useful should an account recovery become necessary. Note from KSN: Keep in mind that alternative 2FA exist, such as OTP or security keys. On top of being more secure than SMS verification, they don't force you to share additional PII with the provider.

Read More on TheHackerNews

Even More on NakedSecurity

iTerm2 Patches Critical Vulnerability Active for 7 Years



The most popular terminal emulator for macOS, iTerm2, has been updated to fix a critical security issue that survived undisclosed for at least seven years. Attackers can achieve remote command execution on systems with a vulnerable iTerm2 version when the application is used to connect to a malicious source.

Tracked as CVE-2019-9535, the vulnerability was discovered following a security audit from Radically Open Security, sponsored by the Mozilla Open Source Support (MOSS) program. Mozilla published a proof-of-concept video showing how connecting to a malicious SSH server resulted in running an arbitrary command (calculator app for demo purposes) on an affected system.

"Typically, this vulnerability would require some degree of user interaction or trickery; but because it can be exploited via commands generally considered safe, there is a high degree of concern about the potential impact," Mozilla warns. George Nachman, iTerm2's developer, today announced patches that fix the vulnerability. Users are encouraged to update to version 3.3.6 or 3.3.7beta1 version.

Read More on BleepingComputer

Even More on TheHackerNews

More #News

- cut1
- Hook, line and sinker: How I fell victim to phishing attacks - again and again
- Apple iTunes and iCloud for Windows 0-Day Exploited in Ransomware Attacks
- Cheating at Professional Poker
- Phishing Incident Exposes Medical, Personal Info of 60K Patients
- Attor, a spy platform with curious GSM fingerprinting
- Most Americans can't recognize 2FA, HTTPS, or private browsing
- Patching as a social responsibility
- TOMS hacker tells people to log off and enjoy a screenless day

- Only 1 in 5 enterprises have DMARC records set up with an enforcement policy
- Thunderbird to add built-in support for OpenPGP email encryption standard
- Researcher Adds $100,000 Worth of Credit to Voi E-Scooter App
- Developers' Code Reuse Security Conundrum: Cut, Paste, Fail
- Imperva blames data breach on stolen AWS API key
- Hacker Selling User Info Stolen From Prostitution Forums
- Nationwide facial recognition ID program underway in France
- 1 Million People Had Their Medical Data Exposed in Tū Ora Breach
- NIST's Zero Trust Taxonomy Introduces Components, Threats and Migration Routes
- FBI warns about attacks that bypass multi-factor authentication (MFA)
- Unpatched VPN Servers Targeted by Nation-State Attackers

#Patch Time!

- Patch Tuesday Lowdown, October 2019 Edition
- SAP Patches Critical Vulnerabilities With October 2019 Security Updates
- New Microsoft NTLM Flaws May Allow Full Domain Compromise
- Microsoft fixes critical remote desktop bug
- These are the Apple macOS Catalina 10.15 security updates you need to know about
- No Patch for Critical Code Execution Flaw Affecting D-Link Routers
- Microsoft Releases the October 2019 Security Updates for Office
- Google Patches Remote Code Execution Bugs in Android 10
- vBulletin Releases Patch Update for New RCE and SQLi Vulnerabilities
- Zero-day published for old Joomla CMS versions
- Signal Rushes to Patch Serious Eavesdropping Vulnerability
- How to Prioritize Vulnerability Patching

#Tech and #Tools

- VM based solution to beat browser fingerprinting
- IAM Least Privilege Policy Generator
- Mapping Windows API's to Sysmon Events
- API Security Tools
- Chrome Enterprise / Ephemeral mode / Password Alert
- Imperva Security Update
- DrSemu - Malware Detection and Classification Tool Based on Dynamic Behavior
- XS-Leak: Leaking IDs using focus
- Simple Trick For Red Teams
- FIDO2: solving the password problem
- FOSS : A poor man's security analysis architecture.
- Revisiting Email Spoofing
- Advisories 1-2: Azure AD and Common WS-Trust MFA Bypass explained
- Pair Locking your iPhone with Configurator 2
- AAPG: [A]ndroid [A]pplication [P]entest [G]uide
- (Super) Magic Hashes
- UK - Change of CCRA Status

- Meterpreter + Donut = Reflectively and Interactively Executing Arbitrary Executables via Shellcode Injection
- No Time to Waste: How Windows 10 Timeline Can Help Forensic Experts

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. 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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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