kindred

Security Newsletter

24 September 2018

Subscribe to this newsletter

Magecart claims another victim in Newegg merchant data theft

Magecart, the notorious hacking group behind the Ticketmaster and British Airways data breaches, has now victimized popular computer hardware and consumer electronics retailer Newegg.

Magecart hacking group managed to infiltrate the Newegg website and steal the credit card details of all customers who entered their payment card information between August 14 and September 18, 2018, according to a joint analysis from Volexity and RiskIQ. The Magecart hacking group, which has been active since 2015, registered a domain called neweggstats.com. Being similar to Newegg's legitimate domain, newegg.com, it was likely registered to appear as a genuine extension of the true domain.

The attack affected both desktop and mobile customers, though it is still unclear how many customers were actually hit by this credit card breach. However, considering that more than 50 million shoppers visit Newegg every month and that the malicious code was there for over one month, it could be assumed that this Magecart newest card skimming campaign has possibly stolen the payment information on millions of Newegg customers, even if only a fraction of those visitors make purchases.

But where would this payload come from? Newegg itself. Around the same day, the cyberattackers were able to infiltrate Newegg systems and drop payment card skimmer code into the e-retailer's checkout process.

How do we solve the problem? There is no silver bullet, but some security measures definitely make it harder for the attacker: 1) Define a (strict) Content-Security-Policy (CSP) 2) Trust your 3rd parties, but verify with Subresource Integrity (SRI) 3) Make sure all assets on sensitive pages use SRI through...CSP.

Read More at ZDNet

Even more at TheHackerNews

Report from RiskIQ

Magecart are coming for you, are you ready?

Cutting room floor

- New XBash malware combines ransomware, coinminer, botnet, and worm features in deadly combo
- Critical Security Update Released for Adobe Reader and Acrobat
- This Windows file may be secretly hoarding your passwords and emails
- 'I am admin' bug turns WD's My Cloud boxes into Everyone's Cloud
- Powerful Android and iOS Spyware Found Deployed in 45 Countries
- Credential Stuffing Attacks Generate Billions of Login Attempts
- Perth Mint Says 3,200 Customers Affected By Data Breach
- Google's Android Team Finds Serious Flaw in Honeywell Devices
- Airline Discovers Trove of Frequent Flyer Accounts Compromised and Posted for Sale Online
- Kraken Cryptor Ransomware Masquerading as SuperAntiSpyware Security Program
- New CSS Attack Restarts an iPhone or Freezes a Mac
- ZDI Exposed Unpatched Microsoft RCE Zero-day Flaw in Public After it Crossed the 120 Days Deadline
- Cloudflare ends CAPTCHA challenges for Tor users
- NSS Labs Sues CrowdStrike, Symantec, ESET, AMTSO for Alleged Testing Conspiracy
- Warning issued as Netflix subscribers hit by phishing attack
- Cybercrime Markets Sell Access to Hacked Sites, Databases

#Tech and #Tools

- Spotify Padlock: Scalable User Privacy
- Kernel Mode Threats & Practical Defenses: Part 1
- Expanding DNSSEC Adoption
- End-to-End Integrity with IPFS
- RPKI and BGP: our path to securing Internet Routing
- AWS SecurityGroup Grapher: Generate a graphical representation of security groups
- Cracking Dropbike: Data Breach and Free Bike Rides
- Why You Shouldn't Store Sensitive Data in JavaScript Files
- XSS Vulnerabilities in Multiple iFrame Busters Affecting Top Tier Sites
- Protecting Mozilla's GitHub Repositories from Malicious Modification
- Breaking The Facebook For Android Application
- Introducing SharpSploit: A C# Post-Exploitation Library
- Pre-Pwned AMI Images in Amazon's AWS public instance store
- Understanding PGP by Simulating it!