



IT Security & Network Security News

Expedia's TripAdvisor Member Data Stolen in Possible SQL Injection Attack

LinkedIn 48 Twitter Facebook 19 +1 0 Share

By: Fahmida Y. Rashid

2011-03-24

Article Rating: ★★★★★ / 6

There are 0 user comments on this IT Security & Network Security News & Reviews story.

The data breach news keeps rolling in, as TripAdvisor, an Expedia company, confirmed attackers had stolen a part of its member e-mail list from the database.

TripAdvisor discovered a data breach in its systems that allowed attackers to grab a portion of the Website's membership list from its database.

The data breach was discovered over the weekend of March 19, and an "unauthorized third party" stole the e-mail list, Steve Kaufer, co-founder and CEO of TripAdvisor, wrote in an email to members on March 24.

The vulnerability has been shut down, and the company is working with law enforcement as well as conducting its own investigation, he said.

TripAdvisor does not collect or store members' credit card or financial information, and member passwords were not stolen, Kaufer said. He said most members won't notice anything as the result of the breach, although some users may receive some spam. The company notified the customers because "it's the right thing to do," he said.

"As a TripAdvisor member, I would want to know," Kaufer said.

If it is true that no passwords were compromised, it is "good news," according to Randy Abrams, director of technical education at ESET's Cyber Threat Analysis Center. "You have to give them credit for getting that part of the security right," Abrams said.

It is not clear at this point when the actual breach and theft occurred, according to TripAdvisor's FAQ page for the incident. However, TripAdvisor will be implementing additional security precautions to prevent another incident, the company promised.

It is also unclear how many users of the 20 million subscribed customers have been affected.

"99.9999% is a portion. 1% is also a portion," said Abrams, noting that the vagueness of the CEO's email makes it seem likely that it was a significant portion. There is also a difference between saying "many users will be unaffected" as opposed to "most users will not be affected," he said.

The "unspecified vulnerability" was likely exploited by a SQL injection attack, Victor Pinenkov, vice president of engineering at Mykonos Software, told eWEEK. Attackers likely entered SQL statements into several input fields on the TripAdvisor site, which when the page was submitted, were sent to the database, Pinenkov said. The database, not realizing it was an illegal request, ran the command and returned the result. The attacker may have just received the data dump right on the page, or used a debug proxy on the computer to intercept the HTTP response from the database, he said.

This sort of data breach is very common across many industries, said Kaufer.

SQL injection is still the No. 1 attack vector, Josh Shaul, CTO of Application Security, told eWEEK. While sometimes the attacks can result from carelessness on the part of the programmer who built the target Website, for the most part, attackers are getting more sophisticated, he said. "SQL injection attacks will continue to be a primary attack vector because they lead an attacker directly to their target, the database," he said.

It is possible that, with the email addresses in hand, attackers will be spamming affected TripAdvisor members. The company also noted the possibility of targeted phishing attacks, where the emails would ask users for more personal

Rate This Article:

Poor Best

E-mail PDF Version

Print

eWEEK Videos Newsbreak Videos All Videos

Today's Featured Video

Understanding Hybrid Routing For Managed DNS

03:43

Watch Now>

Newest Videos

Grid of video thumbnails with titles and durations.

Videos sponsored by IBM

Suggested Related Content:

Articles Labs/How-To

Multimedia

- Visit the Internet Infrastructure Service Center for resources, videos, blogs and polls. (Sponsor)
- Google Wallet Fails to Encrypt Some Payment Data Posing Security
- Adobe Zero-Day Exploit Targeted Defense Contractors (2011-12-07)
- Applications Riddled With SQL Injection, XSS, Remote Code
- Industrial Systems Still Lack Firewalls, Authentication, Basic
- Federal Agency Needed to Take Charge of Nation's Power Grid, Says
- Maine, Play.com, GSN Customers Hit by Third-Party Data Breach (2011-03-
- Denial of Service Most Common Attack Vector in Second Half

AdChoices

10-TB Solid State Disk

eMLC, 320,000 IOPS, 4-GB/s, 1U The World's Fastest Storage® by TMS

RamSan.com/products/R...

Data Security

New Technologies from Oracle. Learn More. Free Download.

www.quberasolutions.com

Cloud configuration

High volume configuration. Requires a new approach. Download Puppet

www.PuppetLabs.com/Cl...

IT Security Flash Drive

The World's Most Secure Flash Drive With Advanced Encryption Technology

IronKey.com

SUBSCRIBE TO eWEEK

SONY VAIO - Official Site

Smart performance w/Intel® Core™ i7 processor laptops. Free shipping. store.sony.com/VAIO

information such as credit card information, bank account information, passwords and ID numbers.

Attackers can also refer to a list of frequently used passwords and then work through the email list to see if any of these TripAdvisor customers use the same weak passwords on other online accounts, including Facebook, Twitter and e-commerce sites, Shaul said.

Since the members are all from TripAdvisor's database, it is likely that the phishing attacks may somehow reference TripAdvisor, such as a security warning asking users to log in to protect and check their account or to click on a link to "reset" the password for security purposes. Spam messages may even claim special advertising offers exclusive to TripAdvisor members. TripAdvisor warned users to be on the lookout for unexpected messages, mail with misspelling or grammatical errors, or "alarmist" emails.

TripAdvisor will never ask for passwords or sensitive information over email, the company said.

Even though TripAdvisor is based in the United States, its client base is international.

LinkedIn 48 Facebook 19 +1 0 Share

smarter technology Take your IT strategy to the next level. VISIT SMARTER TECH

Post a new comment Login Post

0 Comments

>>> More IT Security & Network Security News & Reviews Articles >>> More By Fahmida Y. Rashid

Email Article To Friend ? Print Version Of Article ? PDF Version Of Article

FEATURED SPONSOR VIDEOS

- Benefits of Workload Optimization
What Smart Companies MUST Learn from Gaming
Advances in Authentication
Vertical Markets Benefit from Workload Optimization
View More Videos

FEATURED SPONSOR MESSAGE

Internet Infrastructure Service Center
Visit the Internet Infrastructure Service Center to cast your vote on the infrastructure issues IT professionals face today.
Click Here

Brought to you by smarter technology enterprise

Brought to you by



- NetApp's Mendoza discusses how MLB utilizes data
Managing Regulatory Change in 2011 and Beyond
New expert blog about automating and improving business decisions.
Deliver business data to iPads and iPhones
Developers—learn how Web apps can win Ultrabooks
Get 3X Performance with Check Point Appliances
Keep your business

Magazine Newsletters Feeds Facebook Twitter Widget

SPEED MATTERS It's time to ditch your antivirus TRY VIPRE ANTIVIRUS BUSINESS FREE 30-DAY TRIAL

SUBSCRIBE APPLY FOR A FREE SUBSCRIPTION BELOW: First Name: Last Name: Title: Company: Address: City: State: Zip Code: Email: SUBSCRIBE



- > Try digital eWEEK
> Renew today
> Subscription help
> MORE FREE SUBSCRIPTIONS

Marketplace (Sponsored Links)

Real-time insights from Google Analytics
Simple, Secure Sharing From Anywhere
Simple, Secure Sharing From Anywhere

Spam & Virus Firewall www.barracudanetworks.com Real-Time Protection with Lowest False Positives. Free Eval Units!

AdChoices