TIPS & TRICKS

Top Security Tips from Cyber Security Experts

- **Use a VPN connection**, whether you're on a corporate network or a public wired or Wi-Fi network. Most corporations obviously have VPN clients for their users but employ VPN connections even outside of work—including on mobile devices.

- **Keep all applications up-to-date** with the latest patches and use a less-targeted browser such as Chrome or Firefox.

- **Create very strong and complex passwords** and change them often, and never, ever reuse a password on another site or account.

- **PUAs (Potentially Unwanted Applications)** are the new foemen in the online realm.

- Free software always come at a price, most frequently by side installing adware, browser extensions or other software you didn't ask for. For that matter, things just worsened last week, when a notorious torrent client started to use customers' computers for bit coin mining.

- **Mobile devices are an open gate to our privacy, secrets, and money (mobile banking).** Be very careful what apps you choose to install and pay special attention to what permissions each app is requesting. For instance, it doesn't quite make sense for a weather app to demand access to your photos, does it?

- **Ask loudly for your right to privacy.** Don't ever say **I have nothing to hide**, because that's equivalent to **I don't care about this right**.

- **Think twice before clicking on links found in emails, especially if you don't know the sender.** Whether you're at home or at work, chances are, you'll receive emails from time to time that are not quite what they seem. Cyber criminals often create convincing emails that appear to come from bank, Credit Card Company and other popular websites that hold financial or other sensitive data.

- **Be careful what you download and ask questions about the site you are downloading from.** We live in a digital age in which we can download just about anything we want to watch, listen to or use… and have access to it almost immediately
  .

- **Layered security is important!** Run dedicated anti-malware alongside your traditional anti-virus solution. Don't forget to keep backups as well.

- **Consider yourself a target for hackers** when using your computer and think about what you are doing. In today's security landscape, we need to acknowledge that sensitive information and private data is always under threat from cyber-criminals.

Source

KNOWLEDGE ARTICLES

Preventing Data Theft

Make Sure Sensitive Information is Secure

Just as you might lock a cupboard or a room in the house to keep your belongings safe, so you should restrict access to certain parts of your computer system. Check out our article on Why it's Important to Restrict Access to Your Data.

Protect Against Malicious Software

Viruses, spyware, ransom ware and other malware (malicious software) can all pose a risk to your business. Make sure you have anti-virus software and that it's up to date. Learn more about Anti-virus software.

Control Physical Access

Be aware who has physical access to your office space and devices. Could someone access or steal your computer? Make sure your computers are away from public access. Consider using a cable lock on your computer or laptop – they work just like a bicycle lock, making it harder for the opportunist thief.

If you or your staff works from home, consider having a separate computer for business. Cyber criminals often focus on broadband connections that are "always on", as well as chat sites, games or file-sharing applications. Having a separate work computer can help to quarantine your precious business data from these risks.

Ensure Every Device Requires Some Form of Identification

Biometric authentication such as fingerprint scanners can be extremely useful, as they mean one less password to remember and unlike passwords they can't be guessed or stolen. If your devices don't have these capabilities, then passwords or PINs are the next most likely option (just make sure passwords are strong). It's important to encourage users to have different passwords for different devices and systems. That way if their password in one system is compromised all your systems are not at risk.

Use Only Secure Networks

Your company network should be secure - make sure you use firewalls. Also consider whether staff accesses your network remotely - do they use a VPN (virtual private network)? Is your workplace's Wi-Fi secure? Do staffs use Wi-Fi when away from the office, such as at home, or in cafes and airports?

Train Your Employees

They often lack the basic awareness of data security and how hackers work. Employees without this knowledge often make innocent mistakes that result in data breaches. Educate them not only things like not sharing passwords, scanning USB drives, being wary of attachments and clicking links, but also on phishing, ransom ware, viruses and other risks. Social engineering is also growing threat for small businesses.

Source

NEWS & ALERTS

US Postal Service suffers data breach that exposed 60 million users' data

- The flaw could allow hackers to modify users' account details without their knowledge or consent.
- The breach was caused by a vulnerable API that was a part of the USPS 'Informed Visibility' program, which has been designed to simplify the job of mail senders.

The US Postal Service (USPS) suffered a data breach that may have exposed the personal information of around 60 million users. USPS issued out a patch to a year-old API flaw that allowed anyone with a account on usps.com to view the accounts of around 60 million other users. The flaw could also allow hackers to modify users' account details without their knowledge or consent.

According to a report by KrebsOnSecurity, the flaw was first discovered by an independent security researcher more than a year ago.

Where does the flaw reside?

The API in question is a part of the USPS 'Informed Visibility' program, which has been designed to simplify the job of mail senders. The program provides bulk mail senders access to real-time tracking data about their packages and mail campaigns.

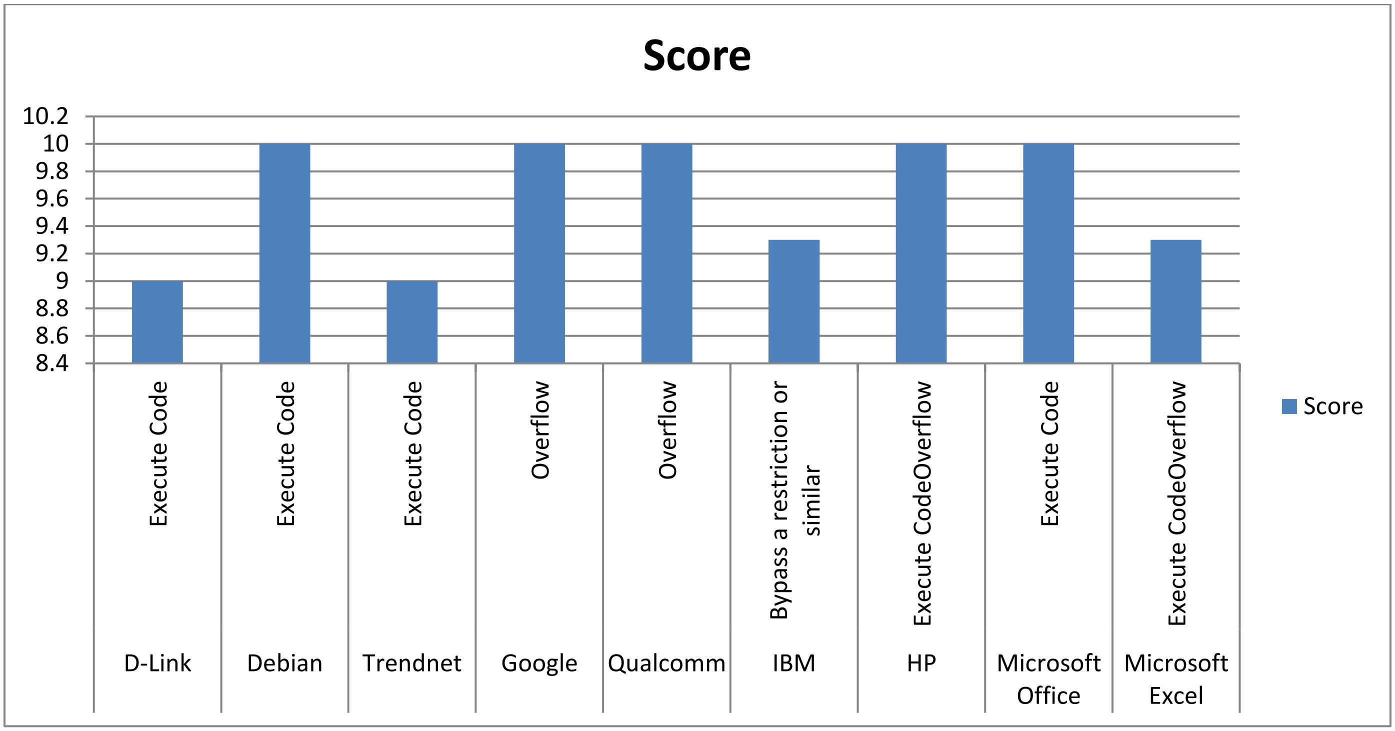
By exploiting the API's wildcard search parameter, hackers could not only access the tracking data of customers, but also their email address, usernames, user IDs, account numbers, street addresses, phone numbers, mailing campaign data and more.

What is more, no special hacking tool was required to exploit the API's flaw. A basic understanding of how to modify the parameters in the web browser console was enough to pull out a stream of confidential data of users from the site.

"This is not even Information Security 101, this is Information Security 1, which is to implement access control," Nicholas Weaver, a researcher at the International Computer Science Institute, told Brian Krebs. "It seems like the only access control they had in place been that you were logged in at all. And if you can access other people's' data because they aren't enforcing access controls on reading that data, it's catastrophically bad and I'm willing to bet they're not enforcing controls on writing to that data as well."

Source

VULNERABILITIES IN LIMELIGHT


Score
Execute Code
D-Link
Execute Code
Debian
Execute Code
Trendnet
Overflow
Google
Overflow
Qualcomm
Bypass a restriction or similar
IBM
Execute CodeOverflow
HP
Execute Code
Microsoft Office
Execute CodeOverflow
Microsoft Excel
Score