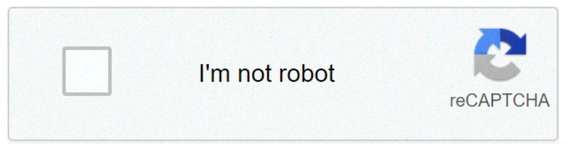

Continue

Vulnerability in computer security

Even if you use the "incognito" setting on your browser, your personal and search data are still being collected at an alarming rate. Private search engines and browsers aim to lessen your digital footprint.By Dave Roos Even if you use the "incognito" setting on your browser, your personal and search data are still being collected at an alarming rate. Private search engines and browsers aim to lessen your digital footprint.By Dave Roos (Image credit: OpturaDesign / Shutterstock.com) UPDATE: SaferVPN has told TechRadar Pro that the company has now released version 5.0.5.0 for Windows, which addresses CVE-2020-26050 and includes an update of the OpenSSL library.ORIGINAL: A security researcher has discovered a new vulnerability in the VPN service SaferVPN that could allow for local privilege escalation on Windows systems.The local privilege escalation vulnerability was discovered by a researcher known as nmht3t who previously disclosed the fact that SaferVPN silently fixed a DoS vulnerability in its VPN client last September. In a new blog post on Medium, mmht3t revealed why he chose to publicly disclose his latest discovery, saying:“SaferVPN does not fix this vulnerability even after a 90-day disclosure deadline. Therefore, there is no patch available at the moment for this product. In order to inform the users of the vulnerability, I decided to publicly disclose the vulnerability.”Security researchers often give companies a 90-day deadline to fix any vulnerabilities before they disclose them publicly. As SaferVPN failed to patch this latest vulnerability in a timely manner, mmht3t felt it was in the best interest of the company's users to warn them about it.According to mmht3t's vulnerability summary, when SaferVPN attempts to connect to a VPN server it spawns the OpenVPN executable in the context of NT AUTHORITY\SYSTEM. The service's VPN client then tries to load an openssl.cnf configuration file from a non-existing folder (C:\etc\ssl\openssl.cnf).However, as a low-privileged users is able to create folders under C:\ on Windows, it's possible for them to create the appropriate path and place a crafted openssl.cnf file in it. Once OpenVPN starts in SaferVPN, this file can load a malicious OpenSSL engine library which results in arbitrary code execution as SYSTEM.SaferVPN versions 5.0.3.3 to 5.04.15 are vulnerable to this local privilege escalation flaw tracked as CVE-2020–26050.Mmht3t first discovered this vulnerability earlier this year and they sent the details of the vulnerability to SaferVPN in July. After a follow up with no response from the company and informing them that the 90-day disclosure deadline was approaching, mmht3t decided to make their findings public in January.We've also highlighted the best VPN Problems with security seem to pop up all the time—from an easy to hack router to apps that leak your data into the world. Thankfully, it's pretty easy to protect yourself. Here's how to do it. Unless you keep up to date on all the security news, it's easy to miss a bit here and there about what has been exploited and what hasn't. We're all vulnerable at some point, and if you haven't touched the settings on your computer since you took it out of the box, it might be time to take another look.Already know about these security holes and have them patched up? Good for you! Send this along to your friends who don't to help keep them safe.UPnP Allows Access to Your Gear from Outside SourcesG/O Media may get a commissionBuy for $43 at StackSocialUPnP (Universal Plug and Play), a component meant to make devices like routers, printers, and media players easy to discover on a network, has been accused of having security holes for a long time, but this week the US Government suggested you disable it yet again. The most recent study suggests 40 million to 80 million network-enabled devices responded to discovery requests from the internet and are vulnerable to an attack that gives hackers access to webcams, printers, passwords, and more. This means routers and devices with the bug can be accessed from the internet to remotely screw with your system even if you don't have malware installed.The good news is that most of the affected hardware is old, and the problem likely isn't as widespread as it seems. That said, in the case of most devices, you can turn UPnP off in the settings (look in your manual for directions). The UPnP setting on your router doesn't have anything to do with the protocol that lets you stream media over a network, print from inside the network, or anything similar. Turning it off on the router level only blocks you from controlling these devices over the internet, which most people don't need to do.Dear Lifehacker, I'm tired of transferring my movies and TV shows to my PlayStation 3's hard drive…Read moreTo turn it off on a router level, you pop into the admin page and disable UPnP. If you want to check your hardware, security site Rapid7 has made a tool to scan devices on your network.Most routers come with some kind of administrative website that you access by typing their IP…Read moreAs far as security risks go, this one's easy to fix and it's not going to affect a lot of people these days. The rest of these are much worse.WEP/WPA Passwords on Your Router Are Easy to CrackChances are that your router is using either a WPA (Wi-Fi Protected Access) password or a WEP (Wired Equivalent Privacy) password. Unfortunetly, it's pretty simple to crack a Wi-Fi network's WPA password and a WEP password.Your Wi-Fi network is your conveniently wireless gateway to the internet, and since you're not keen Read moreBoth of these vulnerabilities exist for different reasons. In the case of WEP, it's as simple as cracking the password with an automated encyrption program (and a lot of time), while in WPA, it's more about a vulnerability in WPS (Wi-fi Protected Setup) on certain routers. This can be corrected by turning WPS off. If you can't turn WPS off, you can install DD-WRT or Tomato so you can. DD-WRT should add a nice security layer to your home network.Of all the great DIY projects at this year's Maker Faire, the one project that really caught my eye Read moreBrowsing Without HTTPS Leaves Your Vulnerable to SnoopersHTTP Secure is the protocol used to secure everything that you send online that's important. This includes your bank information, social networks, and just about everything else that needs security. For your home network, you can simply install the HTTPS browser extension that ensures you'll always use the secure version of a site so your data doesn't fall into the wrong hands. Without HTTPS, your personal data is far more likely to fall through a security hole and into the hands of some nefarious person.Chrome/Firefox: HTTPS Everywhere, the browser extension that keeps your data from falling into the…Read moreWhile it's important to use HTTPS at home, it's far more important to always use it on public Wi-Fi. At places like hotels, airports, or libraries, someone is probably snooping out your passwords. Your best solution for public Wi-Fi is to use a VPN (virtual private network) to route your traffic safely and securely. Public Wi-Fi networks—like those in coffee shops or hotels—are not nearly as safe as you think….Read moreAll the Apps, Software, and Websites You Use Might Accidentally Leak DataIt happens time and time again. A hacker finds an exploit, and suddenly all your favorite software and web sites are vulnerable to people snagging your passwords. This might make your entire system insecure, it may give your passwords away, or they're leaking your personal data like name and address. This happens with Java constantly, but it has happened to pretty much everyone at some point, including: Mega, Google Wallet, Apple, Skype, Path, Zappos, LinkedIn, and Facebook. One million Apple UDIDs (Universal Device IDs) were released to the public today, along with…Read moreFirst off, you need to keep your software up to date. This means both your operating system and your mobile software. Generally, when your data is leaked, someone notices, and the software is patched up right away. When you're home visiting the family, often times you'll find yourself updating a few computers…Read moreIt's not exactly the perfect solution, but since the security holes are on the service or software side, it's all you can do. That said, make sure you have: two-factor authentication enabled where you can, you use a different password for every site, and use a a password system like LastPass to ensure your leaked data doesn't reveal enough information to get your login information for another service.Two-factor authentication is one of the best things you can do to make sure your accounts don't get Read moreStrong Passwords Aren't Enough to Protect Against EverythingWhen it boils down to it, a good password only gets you so far. Certain security holes, like social engineering hacks can happen when a skilled hacker bypasses technical protections (like a strong password) to get the information they want from talking to a person—no "real" hacking is required. It's exactly what happened last year when the Apple and Amazon exploits were uncovered in Mat Honan's hack.In short, people are one of the biggest security holes in the larger chain. Hackers can use psychological tricks to get your information, they might pose as someone important, as a Facebook friend, or even as you when talking with customer support. With a little information, they can then gain access to your account. If that account uses the same password as everywhere else, they essentially get access to everything you do. Thankfully, you can protect yourself with a few simple tips.Dear Lifehacker, My passwords are strong, but if hackers can convince tech support into thinking…Read moreThe main goal is to make sure you don't have all your eggs in one basket. That means if someone gets one password to one site, they can't get in elsewhere. So, never use the same password more than once, use two-factor authentication, get creative with your security questions, and monitor your accounts.You should read Mat Honan's heartbreaking tale of a hack attack and the ensuing discussion on…Read morePlugging up these security holes isn't exactly a fun way to spend an afternoon, but it's certainly more entertaining than waking up one morning to find someone has stolen your identity. It's also a pretty easy process, and once you're set up you don't need to do much else. With the adverse accrescent array of cyber threats, internet security suites have become a necessary tool for safeguarding your devices. It's vital to note that an antivirus (AV) software offers a mere level of protection for your system. On the other hand, an internet security software has multiple programs accessed by a single interface and are thus commonly referred to as suites. They can scan files and software, monitor internet activity, and perform vulnerability searches all by the click of a button. Cyberattacks have made some antivirus-type security solutions useless. There are major antivirus software offering a fitting protection system against malicious attacks like malware but become obsolete when faced with attacks from hackers. An internet security software is a more superior tool when it comes to safeguarding your devices against phishing, spam, spyware, and phishing. But with tons of alternatives out there, where do you begin? Below are our top 10 best internet security software options for you to try depending on your needs. The Symantec Norton Security Deluxe is widely known to outperform its competitors in terms of malware protection, privacy bundles, and special ransomware protection. This software has more than 1,250 5-star reviews from users who love how it's easy-to-install and ease of performing configurations. It's highly compatible with various operating systems (Windows) and devices like Mac or Android systems. With its excellent scanning speed, you can be assured of 100 percent virus removal within the shortest time possible. Other features include a 25GB cloud backup space and a sophisticated firewall. A reasonable price range doesn't necessarily mean inadequate features. On the contrary, Webroot Internet Security Plus with Antivirus Protection proves you can have a fantastic internet security software at a fair price. This cloud-based software offers an all-inclusive internet security protection from viruses and malware. It safeguards information like passwords and account numbers from hackers while blocking phishing and ransomware threats. More than 750 users have given it a 5-star rating due to its ease-of-use and value for money. At its core, Avast Premium Security 2020 features several layers of AI-enhanced virus protection and malware detecting sensors to safeguard your devices against any cyberattacks. This version offers total protection from ransomware, trojans, crypto miners, and spyware making it the ideal internet security software for personal use (one device). It has antispam and anti-phishing capabilities and a sophisticated firewall to prevent hackers from gaining your data and resources. Sandbox is a new feature in this version that allows safe testing of potentially harmful applications. Personal data, like bank information and passwords, are some of the things hackers tend to look for when invading your devices. However, Kaspersky Total Security 2020 goes above and beyond to protect yours against such threats. It comes packed with tools like parental controls, anti-theft and webcam protection, and file backup. An added feature is its unlimited password manager. It saves different passwords often used to log into specific websites. It's compatible with many PC and Mac devices and offers excellent security for kids trying to open dangerous resources. For a newbie, installing and operating an internet security software can be tough at the beginning. No need to worry as McAfee Total Protection easy to install and use once you read the instructions. It has a free 24/7 support channel where you can ask for help either through a phone call or a chat session. The software suite features parental controls, antispam protection, and a true key identity manager. This manager helps in creating a list of known devices, which can be accessed through FingerPrint authentication or Face Recognition. Installation is easy as a click of a button as a digital code emailed directly to you after purchasing it, and all you have to do is enter the 25-digit activation code. In a world where kids own mobile devices and have become central to their everyday life, securing such devices from cyberthreats is paramount. The Webroot Internet Security Complete with Antivirus Protection provides safer web browsing for kids by blocking various malicious attempts to steal their information. Thanks to its cloud-based design, it can scan up to five devices for malware and viruses in a matter of seconds and uses little storage space. Your kid's online accounts are safeguarded with secure password encryption. The software can also warn your kids about malicious websites and links before they open/click. The features are compatible with Mac, Windows, and Android. Apart from ransomware, phishing, and viruses, Kaspersky Internet Security 2020 is well renowned for it's Safe Money Technology. This technology has extra layers of protection to stop online theft from your bank or online shop. Users can pay securely online without worrying about been hacked. More notable features include webcam protection, password manager, system watcher, and alerts when your Wi-Fi is at risk. Threats originating from the Dark Web have never been so varied. For this reason, you require a powerful internet security software like the New Norton 360 Deluxe to ensure real-time threat protection is maintained. With the help of LifeLock, this software monitor and informs you when it finds any of your data on the Dark Web. It also has a Secure VPN that allows you to add bank-grade encryption to safeguard your information. If you're looking for the right internet security software for your Windows operating devices, look no further. The NORTON 360 21.0 is compatible with all Windows Operating Systems. It's able to clean up your hard drive and free up space as well as restore lost horsepower to your personal computer. It has an anti-phishing technology to block misleading "phishing" sites set-up to steal your details. Automatic silent updates are necessary to help be prepared for future advanced threats. This software is capable of warning you about social media scams and dubious content. If you're low on cash and would like to purchase an internet security software that offers a 5- device license, try the McAfee 2018 Total Protection. It's compatible with both Windows and Mac operating systems. This version has parental controls to protect your kids against malicious websites, as well as to limit how much time they spend online. It detects and blocks spam at a fast rate and has a file lock to secure your files. It's the best internet security software if you're dealing with unsolicited emails.