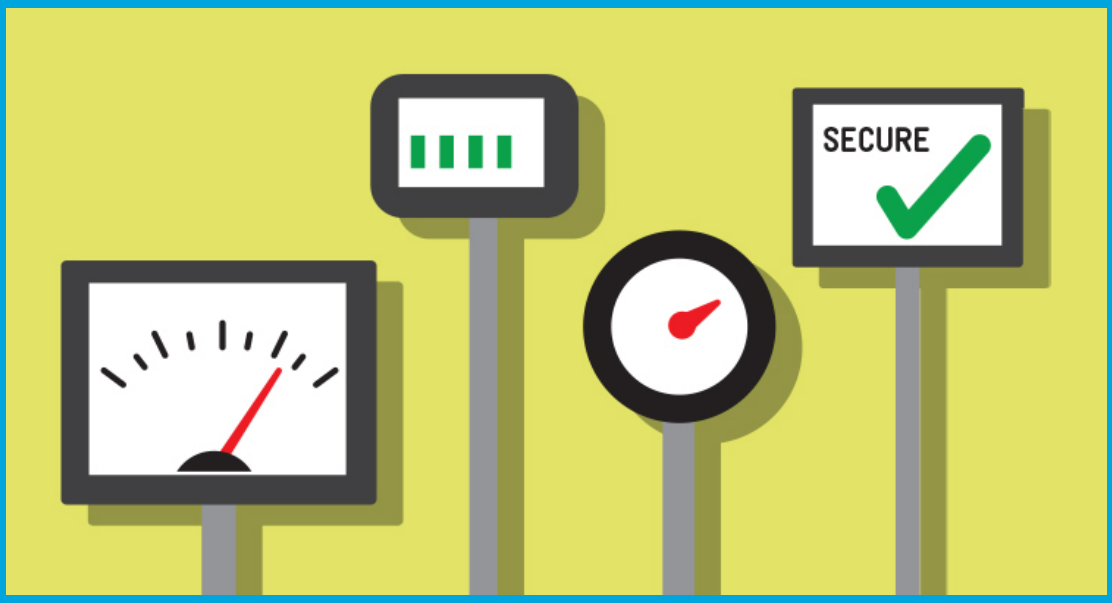
Security Newsletter

17 March 2017

Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security



In a recent CR Consumer Voices survey, 65 percent of Americans told them they are either slightly or not at all confident that their personal data is private and not distributed without their knowledge.

That's why Customer Report is now launching the first phase of a collaborative effort to create a new standard that safeguards consumers' security and privacy. They hope industry will use that standard when building and designing digital products such as connected devices, software, and mobile apps.

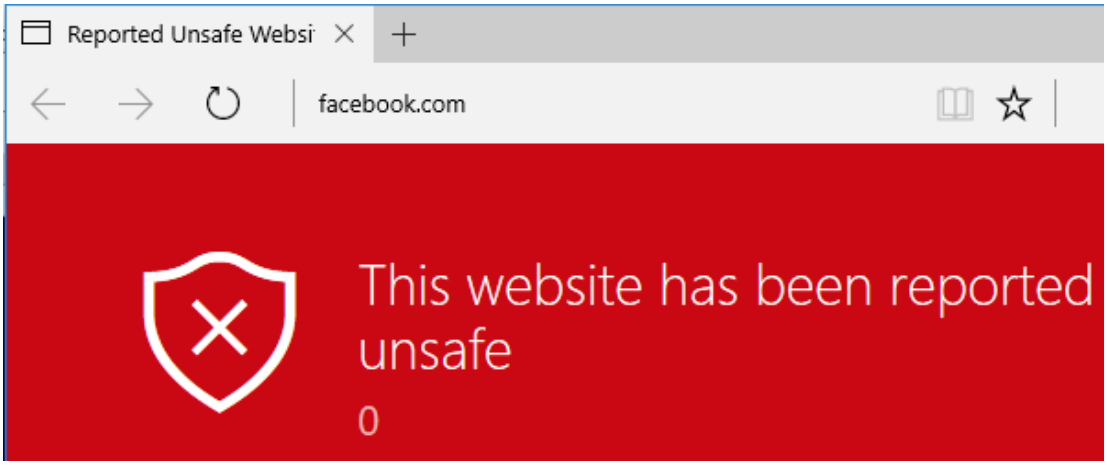
The new standard also calls on companies to delete consumer data from their servers upon request, to protect personal data with encryption as the data is sent through the internet, and to be completely transparent about how personal consumer information is shared with other companies.

Improving products' security and protecting customers' privacy is not just to prevent a hypothetical future brand image impact anymore. Customers are getting more and more interested by how the product they use protect us from the start. Security and Privacy are, finally, being recognized as true added values.

Read More

CR's Guide

Spoofing the Address Bar in Microsoft Edge with the Malware Warning



Over the last few months, we've seen a proliferation of these tech-support scams where users end up "locked" in their browsers with horrible red-screens and messages like "your computer may be at risk". This is not new of course, but scammers are using more and more tricks to fool their victims.

Hackers have recently found a way to spoof the address bar in Microsoft edge, displaying the address of their choice, by abusing how Microsoft Smartscreen operates to warn users about dangerous websites.

This bug was patched on 2017-03-14 but some researchers have found a bypass the same day. This article is a good demonstration of how to evade user input sanitization techniques based on blacklisting.

Read More

Nintendo Switch vulnerable to iOS 9.3 WebKit exploit

A little over a week after the release of Nintendo's new console, the Switch, reputed iOS hacker Luca Todesco has posted an image of an adapted version of his WebKit exploit running on the device.

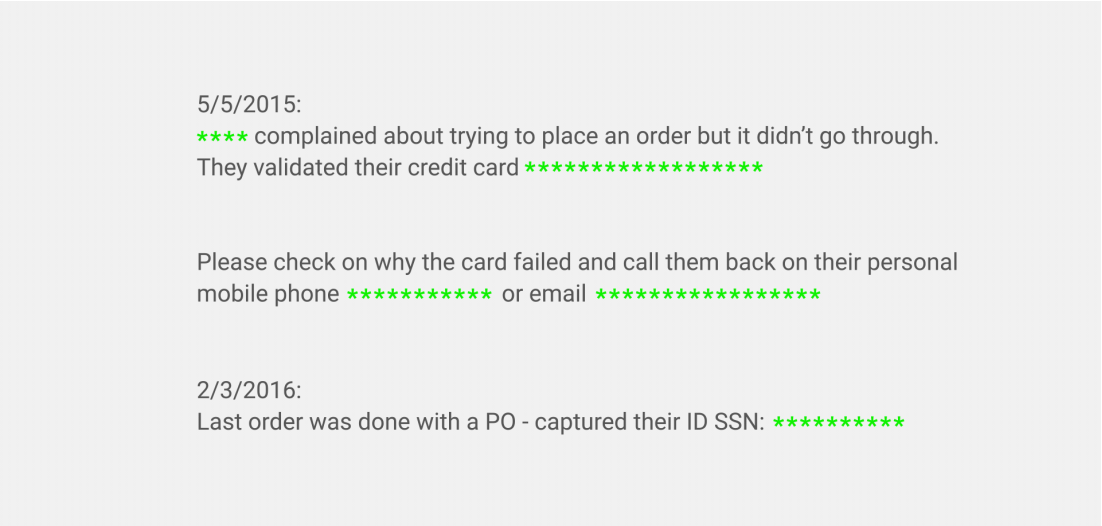
The bug was patched in more recent versions of the open-source WebKit engine, and was likewise fixed up in iOS 9.3.5, but apparently the Nintendo Switch's bundled browser is behind the times and still contains this critical vulnerability.

Whilst this news does not imply that the Switch is close to being fully jailbroken, it is a first step, and is certainly notable in its transference of the underlying bug. It seems slightly lax of Nintendo to have shipped a browser incorporating such a powerful and well-known exploit, but at this point it has only been used to gain code execution within the browser, not over the entire system.

While Nintendo own codebase may be properly implemented following security best practices, heavy use of third party libraries make you vulnerable to other teams' mistakes. That's why it is equally important to monitor the security of your dependencies and update them in a timely manner.

Read More

Bolstering security across Google Cloud



Watch the DLP API filter out sensitive data

This week at Cloud Next '17, Google launched several new features for Google Cloud Platform (GCP) and G Suite that are designed to help safeguard your company's assets and prevent disruption to your business.

Identity-Aware Proxy (IAP) for GCP (now in beta) allows you to manage granular access to applications running on GCP based on risk, rather than the "all-or-nothing" approach of VPN access. **Data Loss Prevention (DLP) API** for GCP (now in beta) lets you scan for more than 40 sensitive data types so you can identify and redact sensitive data.**Security Key Enforcement (SKE)** for GCP and G Suite (now generally available) allows you to require security keys be used as the two-step verification factor for stronger authentication whenever a user signs in.

By baking security into everything they do and offering innovative capabilities that build upon this secure foundation, Google creates many different layers to prevent and defend against attacks and implement enterprise security policies.

Read More

Lip reading: biometrics you can reset just like passwords?

Fingerprint. Voice. Face. Today's smartphones already include a wide variety of biometrics features that allow you to unlock your phone, access apps and even authorize payments. Now, researchers have come up with a new identity authentication system – using lip reading.

This article is a good opportunity to remind readers about the main pitfalls of this authentication method: Accuracy and the capability to recover from "compromised credentials". On the accuracy side, biometrics still have some challenges. First, they have to cope with changes in our body, such as when we are ill, injured – or simply getting older. Biometrics will never give you the definitive "yes" or "no" a password can, you have to finely tune it so that you have low false positive and low false negative. This is what we call FAR (False Acceptance Rate) and FRR (False Rejection Rate). When looking for a new kind of biometrics, always look for those data.

Biometrics also faces another significant obstacle: you can't reset them if they're compromised. You can't change your fingerprints, same for your retina or your voice. Maybe new ideas, such as lip reading, will allow the industry to overcome this issue?

Read More

How online gamers use malware to cheat

We typically think of malware as something used to steal data from corporations or knock down websites in politically motivated attacks. But if you're a gamer, sometimes it's simply a tool for winning.

"I see a lot of different malware at Sophos, and I've also heard a lot about video game cheats. Then I started to dig into cheating, and I found that it's very similar to malware. What I mean by cheat is a software for changing an online, competitive game in real time."

The anti-cheat software developers are following a similar trajectory as that of anti-malware software. Despite its problems, behavioral analysis is taking more of a role in the defensive tools under development, and he has hope that such tools will work better in the near future. He also has hope for the tools under development that incorporate machine learning.

Read More

Adobe fixes 8 Security Vulnerabilities in Adobe Flash Player and Shockwave Player

Adobe has released updates for Adobe Flash Player and Adobe Shockwave Player that resolves a combined 8 security vulnerabilities. Of these 8 vulnerabilities, 7 of them are rated as Critical because they could lead to information disclosure or remote code execution.

A remote code execution vulnerability is particularly worrisome as it could allow attackers to remotely execute command on an affected machine. **This would allow them to execute almost any command, including the downloading and execution of malware**, on the remote computer without the knowledge of the owner.

With Flash and Shockwave being less and less necessary to surf modern website, the best approach is to disable those addons in your browser. At the very least, enable click-to-play for plugins. Same goes to Java of course.

Read More

GitHub Enterprise Remote Code Execution

Everyone uses GitHub. If you have huge amount of green paper or you are very paranoid about your code, you can run your own GitHub. For $2,500 USD per 10 user years you get GitHub Enterprise: A virtual machine containing a fully-featured GitHub instance. Despite a few edge cases that are handled with an occasional GitHub.enterprise? invocation, it runs the same code base as the original.

So let's hack it.

This articles nicely explains how the researcher abused ill-implemented cryptography and Ruby object deserialization routines to perform Remote Code Execution on the Github enterprise server.

Read More

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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.