UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

MARCH 2018 | EDITION 3

IN THIS ISSUE

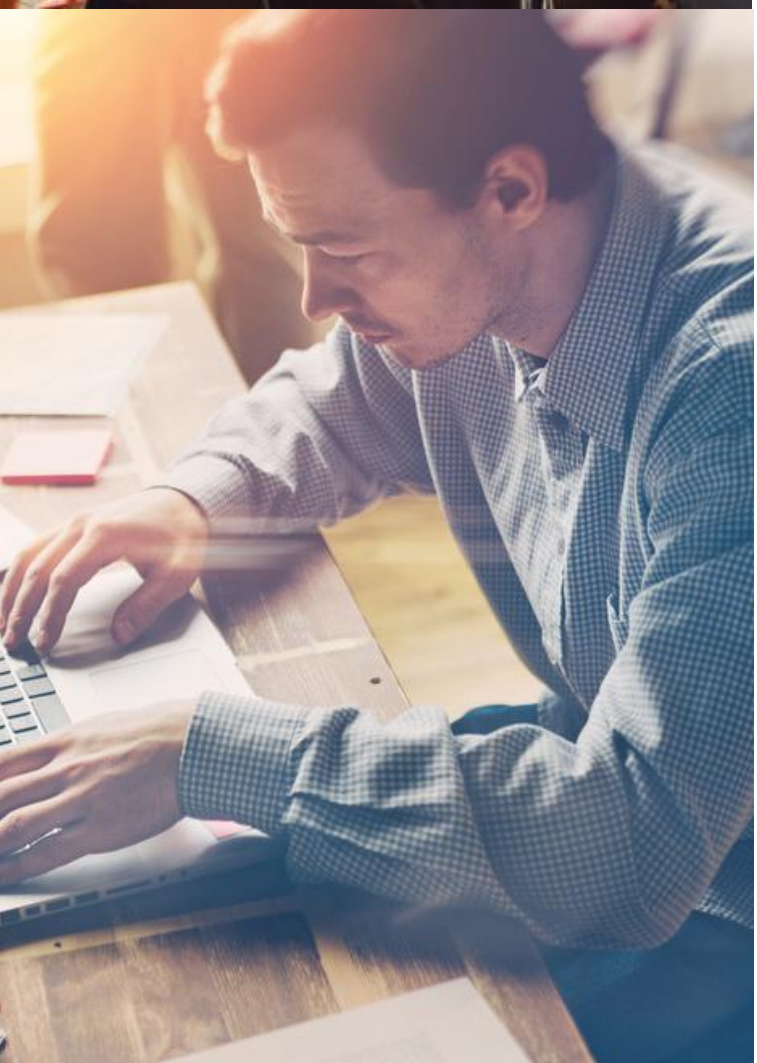
EDITOR'S NOTE

We know that the lack of skilled professionals is a major problem plaguing the cyber security and IT industry. At Cybrary, we're actively working to combat this issue, not just by providing free training, but by matching qualified professionals with cutting-edge companies.

Get access to the most highly vetted talent in the cyber security industry. Industry professionals who are looking to get to the next stage of their career, are learning and assessing their skills on Cybrary, right now.

Join the waitlist to hire Cybrary job candidates. Tenable and Cognizant are already using us. You should too.

Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.



CYBER SECURITY NEWS

#VULNERABILITIES

Most security folks use VPNs to protect their data and online activities, but what if we told you researchers have found critical vulnerabilities in 3 popular VPN services that leak user's real IP addresses and sensitive data? VPNo thank you.

For those unfamiliar, VPNs work by encrypting your data and obscuring your actual IP address. Most people use these services to bypass online censorship and access blocked websites. Researchers hired by privacy firm VPN Mentor discovered that HotSpot Shield, PureVPN, and Zenmate, which combined have millions of customers worldwide, contained vulnerabilities that could compromise user privacy. A report from The Hacker News notes, "After a series of privacy tests on the three VPN services, the team found that all

three VPN services are leaking their users' real IP addresses, which can be used to identify individual users and their actual location."

As of now, the issues in ZenMate and PureVPN have not yet been patched. HotSpot Shield, however, has released fixes to (CVE-2018-7879), (CVE-2018-7878), and (CVE-2018-7880). Executed together, the three flaws could allow a hacker to hijack all traffic, leak your DNS, and leak your real IP address. These vulnerabilities were limited to the free Chrome plug-in and did not affect smartphone apps. Researchers Paulos Yibelo said that the information spilled could allow a third-party to narrow down or even pinpoint where the user is located. This isn't the first time HotSpot Shield has been in hot water.

Cybrarian David Balaban answers the question, 'Why do you need a VPN?'

#PROCESSORS

If your ears are still ringing whenever someone mentions Spectre or Meltdown, it seems we're not rid of these vulnerabilities just yet. Researchers have claimed there are 13 similar vulnerabilities throughout AMD's Ryzen and EPCY processors.

The apparent vulnerabilities could allow attackers to access sensitive data, install malware inside the chip, and gain full access to the systems. Researchers have classified the vulnerabilities into four classes: RYZENFALL, FALLOUT, CHIMERA, and MASTERKEY. These flaws affect a wide-range of servers, workstations, and laptops running the

"The vulnerabilities could allow governments, hostile organizations [sic], or individuals to identify the actual IP address of a user, even with the use of the VPNs."
-VPN Mentor

infected processors. The researchers from CTS-Labs found that the vulnerabilities "defeat AMD's Secure Encrypted Virtualization (SEV) technology and could allow attackers to bypass Microsoft Windows Credential Guard to steal network credentials."

What's worse, the initial discovery led to an even worse realization- there are also two exploitable manufacturer backdoors that could allow for the injection of malicious code inside the chip. It's also worth mentioning that all the vulnerabilities require low privilege access and administrative only in some cases. CTS-Labs gave only 24 hours for AMD to review all the details and respond before going public, despite indicating that the issues could take "several months to fix." In the wake of the Spectre and Meltdown vulnerabilities, researchers say ""We urge the security community to study the security of these devices in depth before allowing them on mission-critical systems that could potentially put lives at risk."

"EPYC servers are in the process of being integrated into data centers around the world, including at Baidu and Microsoft Azure Cloud, and AMD has recently announced that EPYC and Ryzen embedded processors are being sold as high-security solutions for mission-critical aerospace and defense systems"
-CTS-Labs researchers

For full details into Meltdown and Spectre, read this previous edition of UNMASKED.

#LAWSUIT

Finally! Justice for breach victims. A federal judge ruled that those affected by the Yahoo! breach can sue the company.

Back in 2016, Yahoo! announced that a breach of their systems affected over 3 billion users. Since then, U.S. District Judge Lucy Koh

rejected a bid from Verizon Communications, Inc., which bought Yahoo in June, to dismiss several claims including negligence and breach of contract. "The Plaintiffs accused of being too slow to disclose the breaches and thus increased the user's risk of identity theft and requiring them to spend money on credit freeze, monitoring, and other protection services." The judge also said that plaintiffs allegations are sufficient to show they would have behaved differently had defendants disclosed the security weaknesses of the Yahoo Mail Systems. Yahoo! stated in defense of the impending lawsuits that is has been a target of 'relentless criminal attacks.' Lawmakers have since scrutinized Yahoo!'s handling of the breach.

In related industry news, Equifax, responsible for what is being considered one of the largest data breaches in history, is in the spotlight again. Jun Ying, a Former Chief Information Officer, was charged with insider trading. Ying learned of the breach two

weeks before it had been publicly announced. It was then that Ying sold all of his Equifax stock options, worth $950,000, to avoid losses incurred by the announcement of the breach. Equifax reported Ying's trading activity to the government and fired him a month later, but the SEC investigation is still ongoing. "In September, the credit reporting agency disclosed the names of three other Equifax executives who sold shares of the credit bureau worth nearly $2 million shortly after the massive data breach was discovered." It's likely we'll continue to hear about the mishandling of the Yahoo! and Equifax breaches.

For details on the latest update to the Equifax saga, read this recent edition of UNMASKED.

"Ying used confidential information to conclude that his company had suffered a massive data breach, and he dumped his stock before the news went public"
-Richard Best, Director of the SEC Atlanta Regional Office

FACT BYTE

35% OF SURVEY RESPONDENTS REPORT SPENDING AT LEAST $1,000 ANNUALLY IN TRAINING-RELATED EXPENSES

-2018 Cybrary Declassified Report

MEET THE CYBRARIAN

PRIYANK GADA

Priyank has experience as a forensics expert and penetration tester, but frequently shares his knowledge in 0P3N. Now, he also teaches an **Ethical Hacking with Kali Linux Course.**

“Personally, I share my knowledge because I learned everything for free from tutorials that I downloaded. I believe in karma and believe that knowledge should be free. When I first started hacking, there was no one to teach me what is ethical, or what the boundaries are, so I make videos to make sure no one else goes down the bad path.”

START COURSE

TEACH ON CYBRARY

SSCP Practice Test

The SSCP certification strengthens an individual's security posture, proving they have the hands-on technical ability to handle daily procedures which will improve data confidentiality, integrity and availability. This practice test will prepare you to confidently ace the Systems Security Certified Practitioner (SSCP) certification exam.

Get Started

Developing SQL Databases Virtual Lab

The Developing SQL Databases Virtual Lab allows you to gain hands-on skills needed to design database objects, implement programmability objects, manage database concurrency, and optimize your SQL infrastructure, but it will also prepare you to confidently ace the Microsoft 70-762 certification exam.

Dive In

CAREER ROADMAP

If you're waiting until you feel talented enough to make it, you'll never make it."

-Criss Jami

“Organizations keep adding IoT devices to their IT environments with little or no thought about security, or worse, take no time to assess how many IoT devices are touching their networks. In these ways, they’re making it easy for adversaries to take command of the IoT,” the ACR states.

You can earn a badge and a Certificate of Completion when you pass the ACR 2018 Assessment. Simply apply code **ACR2018** to take the assessment free.

Continue Reading **Take Assessment**

Security Auditor

Required Knowledge & skills

Follow the track of an industry leader's job description. Click the buttons below to view courses and supplemental materials that will put you on the path to this career

Correct the errors made by vendors, administrators, and unauthorized users ▶ **CISA**

Excellent analytical, leadership, and conflict resolution skills ▶ **PMP**

Detect, assess, and exploit various types of cybersecurity vulnerabilities ▶ **Certified Ethical Hacker**

Understand government law, policies, and requirements ▶ **Policy Development**

Career Path Beta Program

Cybrary Career Paths is a new program with the main goal of accelerating your journey to a successful technical career by providing training for technical positions with industry leaders like Cognizant.

Apply Today

Inside Cybrary

Shattering the Cyber Security Glass Ceiling

"Companies should not only seek to attract more women, but to retain and promote them, as they should with all employees. Although it may sound easier said than done, it starts with providing skill-based training meant to move all employees progressively down their career path. Adopting a proactive approach where continuous learning is a part of employees expected responsibilities encourages growth and retention."

Read the Full Post

Start a Course