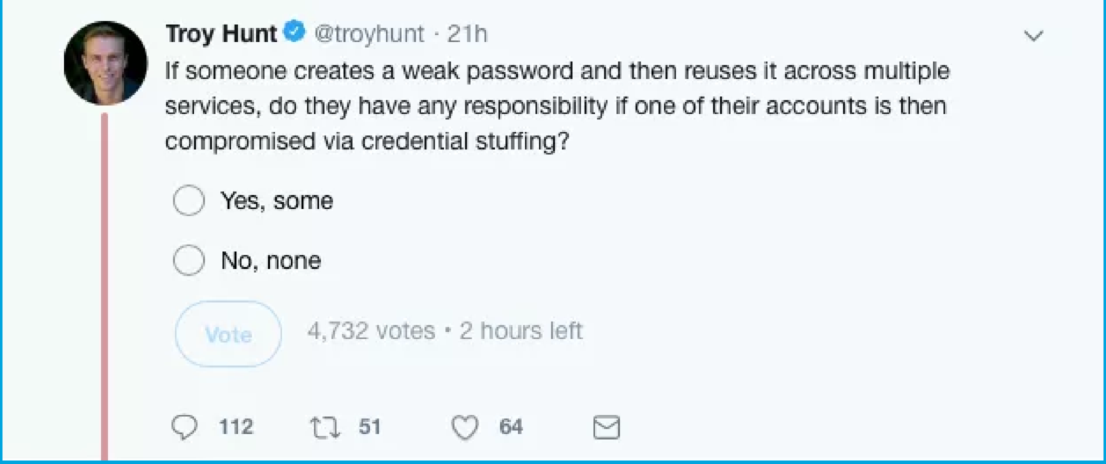
kindred

# Security Newsletter

12 November 2018

Subscribe to this newsletter

## Credential Stuffing - HSBC Bank Alerts US Customers to Data Breach: Who is to blame?



Troy Hunt @troyhunt · 21h

If someone creates a weak password and then reuses it across multiple services, do they have any responsibility if one of their accounts is then compromised via credential stuffing?

○ Yes, some

○ No, none

Vote 4,732 votes • 2 hours left

112 51 64

HSBC bank is warning some of its U.S. customers that their personal data was compromised in a breach, although it says it's detected no signs of fraud. HSBC says the breach appeared to run from Oct. 4 to Oct. 14. After spotting the breach, the bank says in a notification announcement, it "suspended online access to prevent further unauthorized entry" to affected accounts.

The Telegraph reports that HSBC manages about 1.4 million U.S. accounts, meaning 14,000 customers may have been affected. While HSBC has released scant details, Woodward says this breach has all of the hallmarks of a "credential stuffing" attack. Such attacks involve criminals taking usernames, passwords or other personal data that has been stolen or leaked and using it to access a user's account with other sites or services. Millions of such leaked credentials have come to light.

The best defense against credential stuffing attacks is for users to never reuse a password on more than one site. Unfortunately, many users do reuse their credentials. "This is the underlying problem: People have said: 'Hey, I have a favorite password, it's my cat's name and this is the year that it was born; this is fantastic and I'm going to use it everywhere,'" password security expert Troy Hunt.

"This website B didn't necessarily do anything wrong, but now they've got to deal with the risk of ... an attacker logging in with a victim's credentials," Hunt said. "That's a really hard problem. Now, for the most part there was much support for this and clearly very many likes. But there was also a theme that popped up that needs addressing, and it boiled down to this: You're victim blaming.""

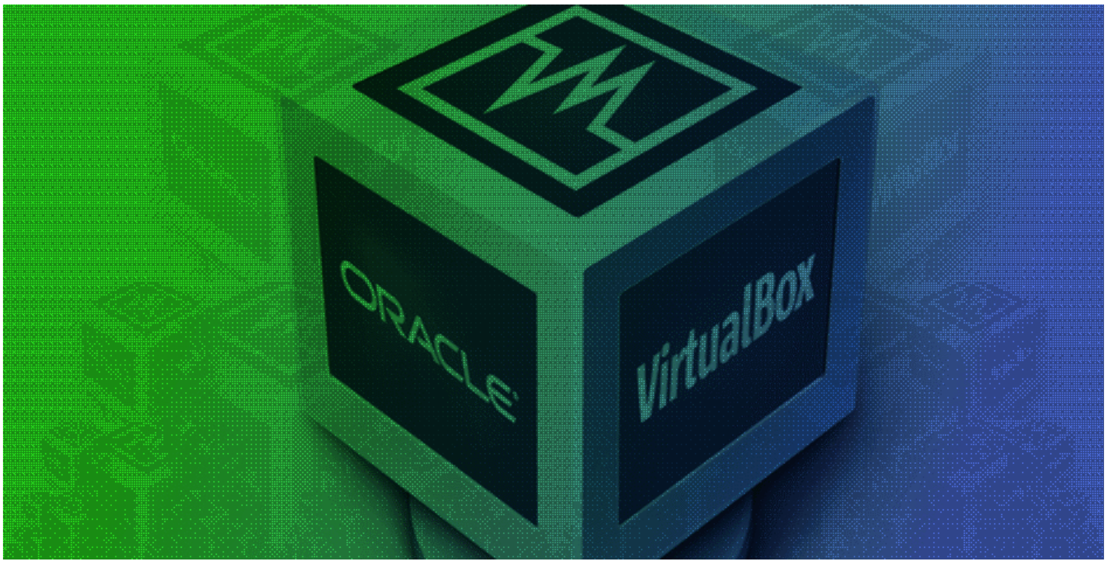
J4vv4d, another well known information security public figure, disagreed with Troy Hunt and thinks what we're lacking is proper awareness and cultural changes, like what happened with car safety. "If you're like me and grew up in the 80's, you'll probably remember going on car trips without wearing seatbelts [...] Fast forward a few decades and it's inconceivable that I would get in a car and not 'clunk clink' [...] But these behavioural changes took decades. There have been sustained awareness campaigns, coupled with increased enforcement to get to the point where it's almost deemed socially unacceptable."

Read More on BankInfoSecurity

Victims Must Share the Blame - Troy Hunt

Victim-blaming is not the right approach - J4vv4d

# VirtualBox zero-day published by disgruntled researcher



A Russian vulnerability researcher and exploit developer has published detailed information about a zero-day vulnerability in VirtualBox. His explanations include step-by-step instructions for exploiting the bug. Exploiting the vulnerability allows an attacker to escape the virtual environment of the guest machine and reach the Ring 3 privilege layer, used for running code from most user programs, with the least privileges.

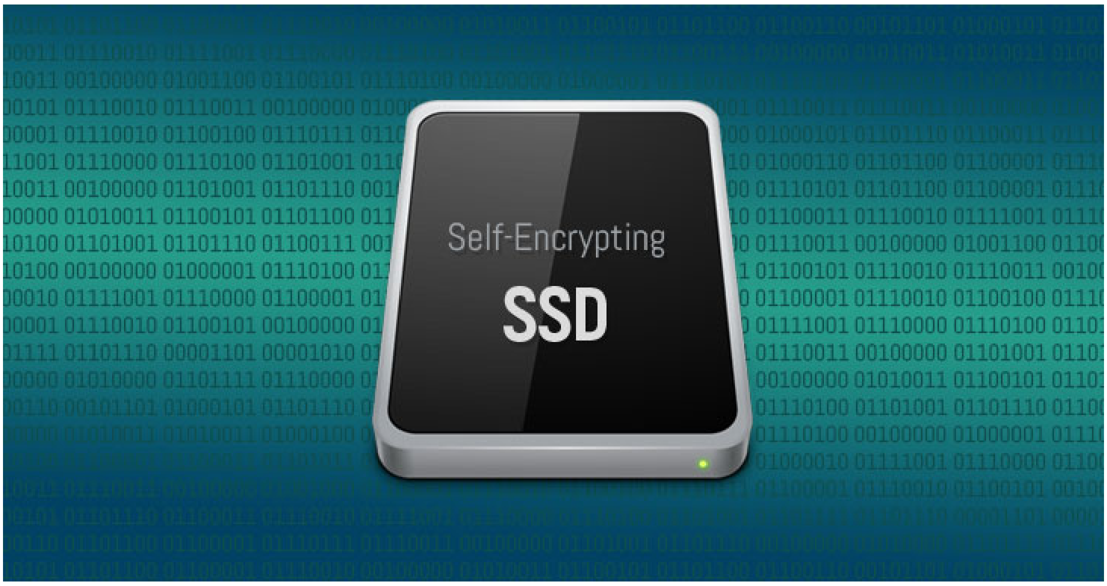
This is not the researcher's first vulnerability disclosure in VirtualBox. Earlier this year, he reported another security bug in VirtualBox. It was reported responsibly for version 5.2.10 of the software. For some reason, though, Oracle fixed the problem silently in version 5.2.18 of its hardware virtualization software and did not give credit to the researcher for finding and reporting the vulnerability.

At the beginning of today's report, Zelnyuk clearly states the reasons that drove him to publicly announcing the full details for the current zero-day, before informing the developer of the issue. Oracle's past reaction to his bug bounty reporting seems to have played a part in this.

Read More on ZDNet

Even More on BleepingComputer

# Flaws in Popular Self-Encrypting SSDs Let Attackers Decrypt Data



Security researchers have discovered multiple critical vulnerabilities in some of the popular self-encrypting solid state drives (SSD) that could allow an attacker to decrypt disk encryption and recover protected data without knowing the password for the disk.

The duo successfully tested their attack against three Crucial models of SSDs—Crucial MX100, MX200, and MX300—and four Samsung SSDs—840 EVO, 850 EVO, T3 Portable, and T5 Portable drives and found at least one critical flaw that breaks the encryption scheme. But researchers warned that many other SSDs may also be at risk. With physical access to the device's debug ports, the researchers were able to reverse engineer the firmware and modify it to decrypt the hardware encrypted data by entering any password.

What's more? Since Windows' built-in BitLocker full-disk encryption software by default uses hardware-based encryption if available, instead of its own software-based encryption algorithms, Windows users relying on BitLocker and using vulnerable drives remain exposed to above-mentioned vulnerabilities. However, you can force BitLocker to use software-based encryption only by changing a setting in Windows Group Policy.

Meijer and Gastel reported the vulnerabilities to Crucial and Samsung before going public with their findings. While Crucial has already released firmware patches for all of its affected drives, Samsung has rolled out security patches for its T3 and T5 Portable SSDs.

Read More on TheHackerNews

Even More on The Register

## More #News and #Leaks

- Steam bug could have given you access to all the CD keys of any game
- Microsoft Releases Info on Protecting BitLocker From DMA Attacks
- Data of nearly 700,000 Amex India customers exposed via unsecured MongoDB server
- Chrome 71 will warn users about websites with shady phone subscription forms
- Cisco accidentally leaked in-house Dirty COW exploit code with biz conf call software
- Bankers Life Hack Affects More Than 566,000
- Busting SIM Swappers and SIM Swap Myths
- Cambodia's ISPs hit by some of the biggest DDoS attacks in the country's history
- Hackers are increasingly destroying logs to hide attacks
- The day computer security turned real: The Morris Worm turns 30
- Who's In Your Online Shopping Cart?
- New Microsoft Edge Browser Zero-Day RCE Exploit in the Works
- Here's Why [Insert Thing Here] Is Not a Password Killer

## #Patch Time!

- Several Vulnerabilities Patched in nginx
- Serious XSS flaw discovered in Evernote for Windows, update now!
- Remote code hijacking flaw in Apache Struts, patch ASAP
- Popular WooCommerce WordPress Plugin Patches Critical Vulnerability
- November Android Security Update Fixes Critical Bugs, Drops Media Library
- ADV180028 | Guidance for configuring BitLocker to enforce software encryption
- WordPress Design Flaw Leads to WooCommerce RCE
- Suricata 4.1 released!
- PoshKatz: PowerShell module for Mimikatz
- Introducing burp-rest-api v2
- Development Of Metasploit Module After 0day
- Pentests in restricted VDI environments

## #Tech and #Tools

- API Security Newsletter
- Operational Challenges in Offensive C#
- Microsoft is Porting Sysinternals Tools to Linux - ProcDump Released
- Cryptocurrency Mining Malware uses Various Evasion Techniques
- Abusing WSL for Evasion
- The New Illustrated TLS Connection - TLS 1.3
- PacketFence v8.2 released

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.

You can access the previous newsletters at https://news.infosecgur.us