kindred

Security Newsletter

18 September 2017

Subscribe to this newsletter

The IoT Attack Vector “BlueBorne” Exposes Almost Every Connected Device

If you are using a Bluetooth enabled device, be it a smartphone, laptop, smart TV or any other IoT device, you are at risk of malware attacks that can carry out remotely to take over your device even without requiring any interaction from your side.

Security researchers have just discovered total 8 zero-day vulnerabilities in Bluetooth protocol that impact more than 5.3 Billion devices—from Android, iOS, Windows and Linux to the Internet of things (IoT) devices—using the short-range wireless communication technology.

Using these vulnerabilities, security researchers at IoT security firm Armis have devised an attack, dubbed BlueBorne, which could allow attackers to completely take over Bluetooth-enabled devices, spread malware, or even establish a "man-in-the-middle" connection to gain access to devices' critical data and networks without requiring any victim interaction.

The security firm responsibly disclosed the vulnerabilities to all the major affected companies a few months ago—including Google, Apple and Microsoft, Samsung and Linux Foundation. Google and Microsoft have already made security patches available to their customers, while Apple iOS devices running the most recent version of its mobile operating system (that is 10.x) are safe.

All iOS devices with 9.3.5 or older versions and over 1.1 Billion active Android devices running older than Marshmallow (6.x) are vulnerable to the BlueBorne attack. Android users need to wait for security patches for their devices, as it depends on your device manufacturers. In the meantime, they can install BlueBorne Vulnerability Scanner app (created by Armis team) from Google Play Store to check if their devices are vulnerable to BlueBorne attack or not. If found vulnerable, you are advised to turn off Bluetooth on your device when not in use.

Even More

Original announcement

CVE List

Equifax data leak could involve 143 million consumers, what to do?

Equifax reports that it discovered the leak on July 29th and took steps to stop the intrusion. It then hired a cybersecurity firm to determine the extent of the intrusion and what damage was done. The company reported that it has involved law enforcement. After investigation, Equifax recently declared that the vulnerability was Apache Struts CVE-2017-5638

The data at risk includes Social Security numbers, birth dates, addresses on 143 million Americans. Equifax also said the breach involved some driver's license numbers (although it didn't say how many or which states might be impacted), credit card numbers for roughly 209,000 U.S. consumers, and "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers.

The breach is not limited to Americans though, Equifax said it believes the intruders got access to "limited personal information for certain UK and Canadian residents." It has not disclosed what information for those residents was at risk or how many from Canada and the UK may be impacted.

While this is not the worst breach of all time by a long shot in terms of pure numbers, this leak is particularly worrisome because Equifax is a credit reporting service. They track a history of your consumer life, credit cards, credit scores and more. This gives the black market a potential gold mine of information about people's financial lives.

Equifax is offering one free year of their credit monitoring service. A credit monitoring can't hurt, but you should not count on it protecting you from identity theft. For that, you need to file a security freeze — also known as a credit freeze — with the four major credit bureaus.

Read More

Credit Freeze - What you should know

Apache Struts 2 Flaws Affect Multiple Cisco Products

After Equifax massive data breach that was believed to be caused due to a vulnerability in Apache Struts, Cisco has initiated an investigation into its products that incorporate a version of the popular Apache Struts2 web application framework.

Multiple Cisco products incorporate a version of the Apache Struts 2 package that is affected by these vulnerabilities.

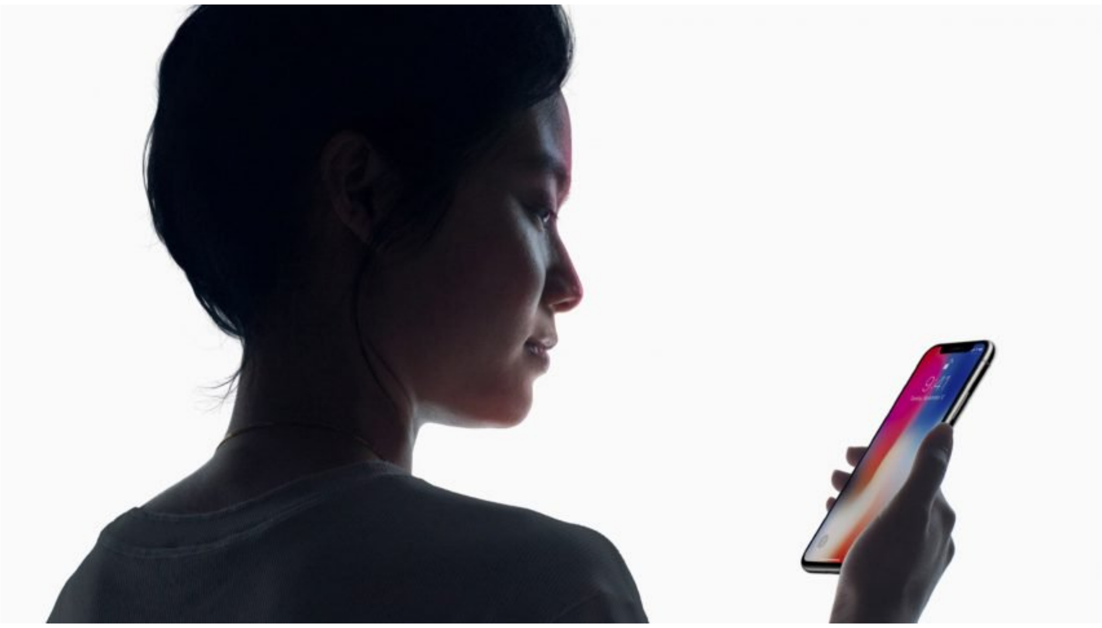
Some of Cisco products including its Digital Media Manager, MXE 3500 Series Media Experience Engines, Network Performance Analysis, Hosted Collaboration Solution for Contact Center, and Unified Contact Center Enterprise have been found vulnerable to multiple Apache Struts flaws.

At the current, there are no software patches to address the vulnerabilities in Cisco products, but the company promised to release updates for affected software which will soon be accessible through the Cisco Bug Search Tool.

Read More

Cisco Advisory Page

Does Apple Face ID make it easier for feds to hack the iPhone X?



The biggest announcement on Tuesday for security folk, facial recognition, may be a double-edged sword. With no home button for Touch ID, Face ID will be the primary way to unlock iPhone X. On the one-hand, the face is a unique identifier and will allow for quick and secure access. On the other, as with fingerprints, past forms of facial biometrics have been exploited with simple tricks, such as holding up a clear picture of the real user.

But Apple appears to have invested seriously in the security of Face ID. Apple senior vice president Phil Schiller said "Face ID learns your face" and can adapt to recognize changes in the user's appearance. The TrueDepth camera system of the iPhone X combines a lot of high-end tech - an infrared camera, proximity and ambient light sensors, as well as a flood illuminator.

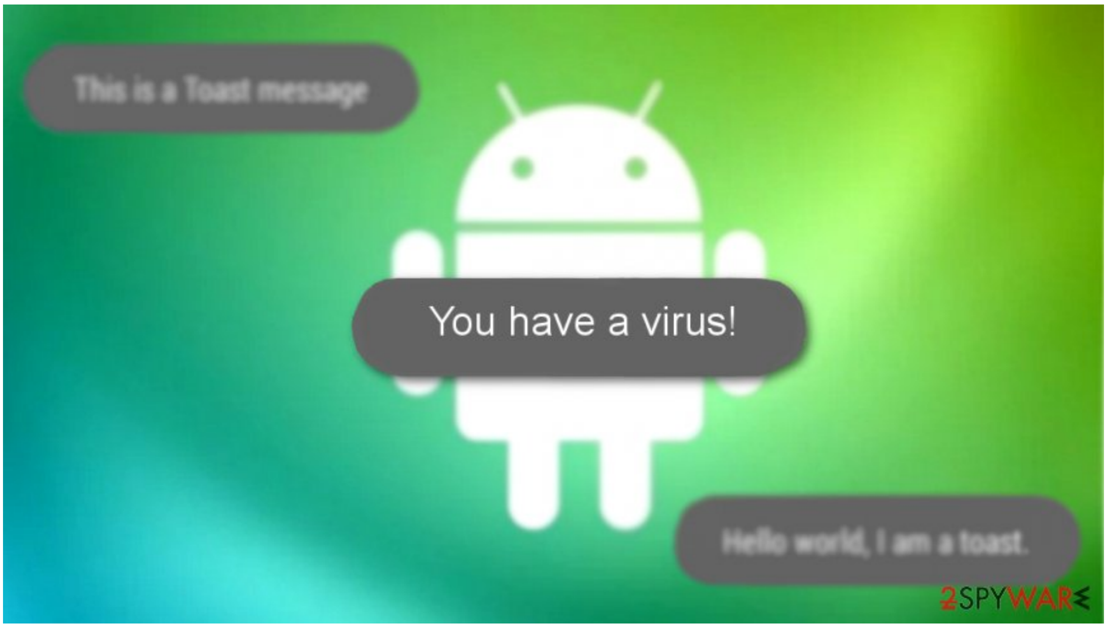
Apple has even worked with Hollywood specialists to test mask attacks. The chance of a random person being able to unlock a device is one in a million, Schiller said. When it comes to law enforcement searches, Face ID could, in one respect, be a boon. It may be easier to force a user into opening their iPhone simply by holding it up to their face when compared to Touch ID, where police have repeatedly tried to force suspects to depress their fingerprint to unlock the phone.

Apple has added an additional login layer in iOS 11 so that when connecting an iPhone to an unknown external PC, an extra passcode is required. For feds then, even if they can unlock the phone, it doesn't mean they can extract the data inside, quite the opposite thanks to iOS 11.

Read More

Even More

Everybody without Android Oreo vulnerable to toast overlay attack



Any unpatched Android phone running a version older than Oreo is going to need patching fairly soon, with researchers turning up a class of vulnerability that lets malware draw fake dialogs so users “okay” their own pwnage.

This vulnerability is a variant of the overlay attack we encountered with the "Cloak and Dagger" vulnerability. It's a straightforward way to trick users: draw a bogus screen for users to click on (for example, to install an app or accept a set of permissions), hiding what's really happening.

Android is supposed to prevent this happening. But the vulnerability turned up by Palo Alto's Unit 42 threat research team bypasses these requirements, by exploiting a notification type called Toast.

Read More

Microsoft says it won't fix kernel flaw allowing to bypass Antivirus scans

A design flaw within the Windows kernel that could stop antivirus software from recognizing malware isn't going to be fixed, Microsoft has said. The issue, spotted this week by enSilo security researcher Omri Misgav, lies within the system call PsSetLoadImageNotifyRoutine, which has been part of Microsoft's operating system since Windows 2000 and is still active in the latest builds.

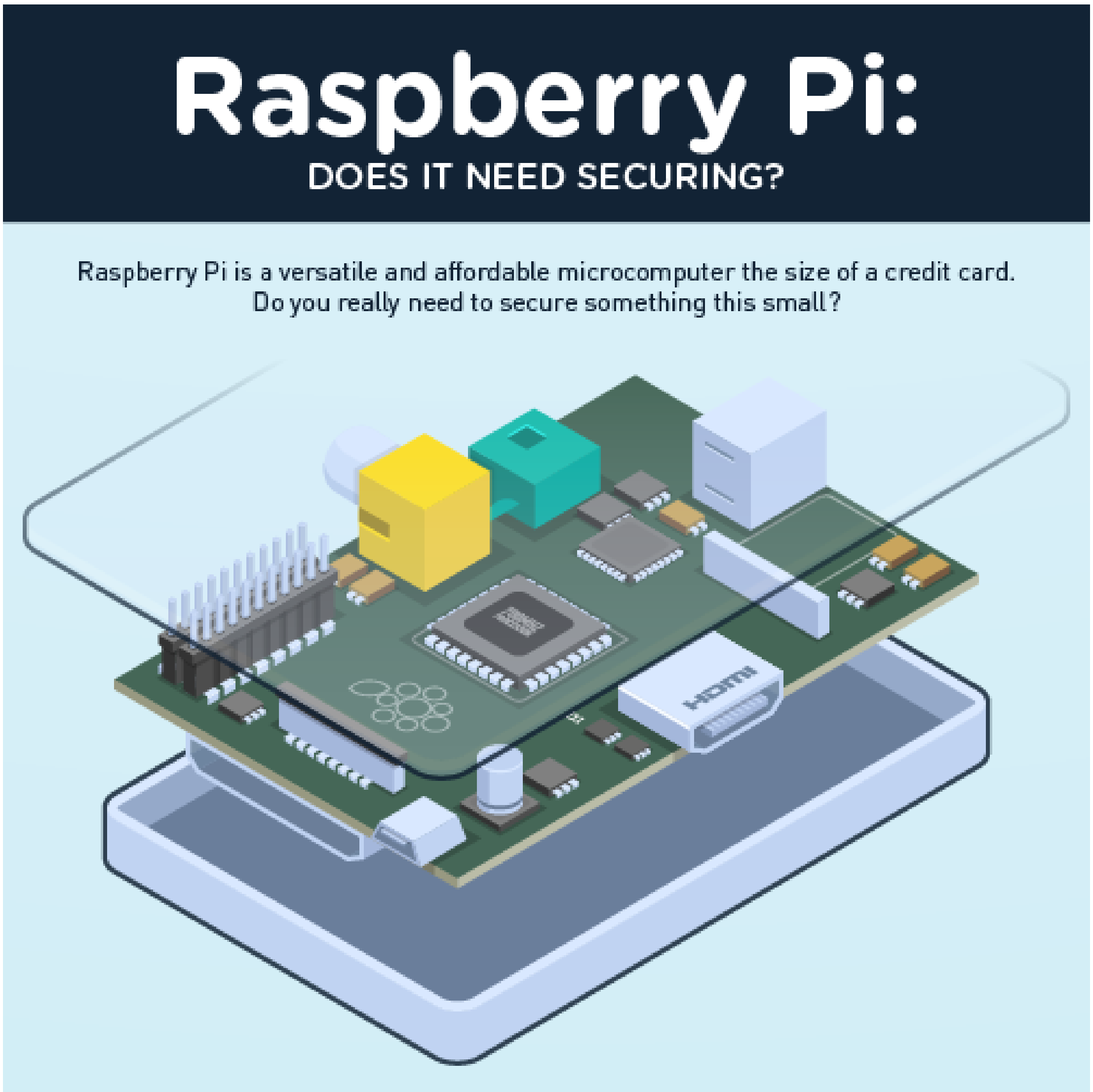
Antivirus tools use PsSetLoadImageNotifyRoutine to check if malicious code has been loaded into memory, but Misgav found that a cunning attacker could use poor coding behind the API to smuggle malware past scanners. Essentially, malware can use the above API to trick the OS into giving malware scanners other files – such as benign executables – to inspect rather than their own malicious code. This would allow software nasties to evade antivirus packages.

After enSilo notified Microsoft about the issue nothing happened. When Redmond's techies did get in contact, they said that they weren't concerned about the issue.

Read More

Original statement

Take These Steps to Secure Your Raspberry Pi Against Attackers


Raspberry Pi:
DOES IT NEED SECURING?
Raspberry Pi is a versatile and affordable microcomputer the size of a credit card.
Do you really need to secure something this small?
HDMI

Raspberry Pi boards are fantastic for any project — they're cheap, easy to use, can run a wide range of possible operating systems. You can use Raspberry Pi boards for all kinds of automation and information gathering projects. But, if you are not careful, your little hobby project might result in a security risk that acts as an entry point into your network.

They can't perform secure booting such as ARM Trustzone, and the SD card and operating system are not easily encrypted. Follow these security tips to safeguard your Pi and other devices on your network.

This guide covers basic security hardening that should be part of any project, tasks such as changing default passwords, securing SSH, configuring the Firewall, ensuring continuous security updates, etc.

Read More

Official documentation

Cutting room floor

- iOS security alert: Your device is transmitting Exchange credentials without any encryption
- Hackers Can Remotely Access Syringe Infusion Pumps to Deliver Fatal Overdoses
- Linux Subsystem on Windows 10 Allows Malware to Become Fully Undetectable
- Researcher reveals D-Link router holes that might never be patched
- Adobe Patches Two Critical RCE Vulnerabilities in Flash Player
- Equifax's credit report monitoring site is also vulnerable to hacking
- Cynic's Guide to the Equifax Breach: Nothing Will Change (and why we need the GDPR)
- Google Is Fighting A Massive Android Malware Outbreak -- Up To 21 Million Victims

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