iPhone Source Code Gets Posted Online in 'Biggest Leak in History'

THOUSANDS OF HACKERS, RUSSIAN AND KOREAN SPIES GOT AHOLD OF IT AND NOW NO APPLE PRODUCT WILL EVER BE SAFE AGAIN

THERE IS "LITERALLY" NOW NOTHING YOU CAN DO ON A PRODUCT RUNNING WINDOWS OR APPLE SOFTWARE THAT CAN'T BE BROKEN INTO VERY EASILY!

Source code for iBoot, one of the most critical iOS programs, was anonymously posted on GitHub.

Lorenzo Franceschi-Bicchierai

Image: Rokas Tenys/Shutterstock

Someone just posted what experts say is the source code for a core component of the iPhone's operating system on GitHub, which could pave the way for hackers and security researchers to find vulnerabilities in iOS and make iPhone jailbreaks easier to achieve.

The GitHub code is labeled "iBoot," which is the part of iOS that is responsible for ensuring a trusted boot of the operating system. In other words, it's the program that loads iOS, the very first process that runs when you turn on your iPhone. It loads and verifies the kernel is properly signed by Apple and then executes it—it's like the iPhone's BIOS.

The code says it's for iOS 9, an older version of the operating system, but portions of it are likely to still be used in iOS 11.

Apple has traditionally been very reluctant to release code to the public, though it has made certain parts of iOS and MacOS open source in recent years. But it has taken particular care to keep iBoot secure and its code private; bugs in the boot process are the most valuable ones if reported to Apple through its bounty program, which values them at a max payment of $200,000.

"This is the biggest leak in history," Jonathan Levin, the author of a series of books on iOS and Mac OSX internals, told me in an online chat, referring to Apple's history. "It's a huge deal."

A screenshot of part of the leaked iBoot source code.

Levin said the code appears to be the real iBoot code because it aligns with code he reverse engineered himself. A second security researcher familiar with iOS also said they believe the code is real. We don't know who is behind the leak. Apple did not respond to a request for comment.

A few hours after the publication of this story, Apple sent a DMCA legal noticedemanding GitHub take down the iBoot code. "The "iBoot" source code is proprietary and it includes Apple's copyright

notice. It is not open-source." This way, Apple indirectly confirmed that the code was real. GitHub took down the code soon after.

Having access to the source code of iBoot gives iOS security researchers a better chance to find vulnerabilities that could lead to compromising or jailbreaking the device, Levin said. That means hackers could have an easier time finding flaws and bugs that could allow them to crack or decrypt an iPhone. And, perhaps, this leak could eventually allow advanced programmers to emulate iOS on non Apple platforms.

Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzo@jabber.ccc.de, or email lorenzo@motherboard.tv

Vulnerabilities in previous versions of iBoot allowed jailbreakers and hackers to brute-force their way through the iPhone's lock screen and decrypt a user's data. But newer iPhones have a chip called the Secure Enclave Processor, which has hardened the security of the device.

For regular users, Levin added, this means that tethered jailbreaks, which require the phone to be connected to a computer when booting, could soon be back. These jailbreaks used to be relatively easy to pull off and were common, but are now extremely hard to

come by on up-to-date iOS devices, which have advanced security mechanisms that make it hard for even highly skilled researchers from even looking for bugs, as they need to first jailbreak the device before beginning to probe the device.

It's these security improvements that have have effectively killed the once popular jailbreak community. Nowadays, finding bugs and vulnerabilities in iOS is something that requires a significant amount of time and resources, making the resulting exploits incredibly valuable. That's why the jailbreaking community gets excited for any leak of source code or any exploit that gets released publicly.

This source code first surfaced last year, posted by a Reddit user called "apple_internals" on the Jailbreak subreddit. That post didn't get much attentionsince the user was new and didn't have enough Reddit karma; the post was quickly buried. Its new availability on GitHub means it's likely circulating widely in the underground jailbreaking community and in iOS hacking circles. "iBoot is the one component Apple has been holding on to, still encrypting its 64 bit image," Levin said. "And now it's wide open in source code form."

NSA Exploits Ported to Work on All Windows Versions Released Since Windows 2000

By **Catalin Cimpanu**

February 5, 2018 07:10 AM 0

A security researcher has ported three leaked NSA exploits to work on all Windows versions released in the past 18 years, starting with Windows 2000.

The three exploits are EternalChampion, EternalRomance, and EternalSynergy; all three leaked last April by a hacking group known as The Shadow Brokers who claimed to have stolen the code from the NSA.

Researcher ports NSA exploits for old&new Windows versions

Several exploits and hacking tools were released in the April 2017 Shadow Brokers dump, the most famous being EternalBlue, the exploit used in the WannaCry, NotPetya, and Bad Rabbit ransomware outbreaks.

While EternalBlue became a favorite tool among malware authors, the Shadow Brokers dump also contained many lesser-known exploits. The reason many of these didn't become popular was that they only worked a small number of Windows versions, and did not support recent Windows distributions.

Now, RiskSense security researcher Sean Dillon (@zerosum0x0) has modified the source code for some of these lesser-known exploits so they would be able to work and run SYSTEM-level code on a wide variety of Windows OS versions.

The researcher has recently merged these modified versions of EternalChampion, EternalRomance, and EternalSynergy into the Metasploit Framework, an open-source penetration testing project.

Dillon has crafted his modified exploits to take advantage of the following vulnerabilities:

CVE	Vulnerability	Exploi
CVE-2017-0143	Type confusion between WriteAndX and Transaction requests	EternalR EternalS
CVE-2017-0146	Race condition with Transaction requests	EternalC EternalS

"Instead of going for shellcode execution, it overwrites the SMB connection session structures to gain Admin/SYSTEM session," Dillon says. "The [Metasploit Framework] module is leaner (stripped down packet count/padding), checks extra named pipes, sprinkles randomness where possible, and has Metasploit's psexec DCERPC implementation bolted onto it."

Exploits work on both 32-bit and 64-bit architectures

Dillon says his modified exploits will work on both 32-bit and 64-bit architectures. He listed the following Windows versions as supported:

```
Windows 2000 SP0 x86
Windows 2000 Professional SP4 x86
Windows 2000 Advanced Server SP4 x86
Windows XP SP0 x86
Windows XP SP1 x86
Windows XP SP2 x86
Windows XP SP3 x86
Windows XP SP2 x64
Windows Server 2003 SP0 x86
Windows Server 2003 SP1 x86
Windows Server 2003 Enterprise SP 2 x86
Windows Server 2003 SP1 x64
Windows Server 2003 R2 SP1 x86
Windows Server 2003 R2 SP2 x86
Windows Vista Home Premium x86
Windows Vista x64
Windows Server 2008 SP1 x86
Windows Server 2008 x64
Windows 7 x86
```

```
Windows 7 Ultimate SP1 x86
Windows 7 Enterprise SP1 x86
Windows 7 SP0 x64
Windows 7 SP1 x64
Windows Server 2008 R2 x64
Windows Server 2008 R2 SP1 x64
Windows 8 x86
Windows 8 x64
Windows Server 2012 x64
Windows 8.1 Enterprise Evaluation 9600 x86
Windows 8.1 SP1 x86
Windows 8.1 x64
Windows 8.1 SP1 x64
Windows Server 2012 R2 x86
Windows Server 2012 R2 Standard 9600 x64
Windows Server 2012 R2 SP1 x64
Windows 10 Enterprise 10.10240 x86
Windows 10 Enterprise 10.10240 x64
Windows 10 10.10586 x86
Windows 10 10.10586 x64
Windows Server 2016 10.10586 x64
Windows 10 10.0.14393 x86
Windows 10 Enterprise Evaluation 10.14393 x64
Windows Server 2016 Data Center 10.14393 x64
```

Several security researchers have independently confirmed Dillon's exploit code works on these Windows versions.

> *exploit/windows/smb/ms17_010_psexec and auxiliary/admin/smb/ms17_010_command are now surely two of the most vigorously tested modules in all of @Metasploit. Thanks to everyone who helped! Should land to master branch soon… pic.twitter.com/NKy8nopF9p*
>
> — zəɹosum0x0 (@zerosum0x0) February 2, 2018

Nothing new. NSA exploits ported in the past.

Part of Dillon's code uses a previous port of the EternalSynergy exploit created by security researcher Worawit Wang. Bleeping Computer previously covered in an article how Wang ported EternalSynergy to work on newer Windows versions.

In June 2017, Dillon also ported the EternalBlue exploit to work on Windows 10. Dillon also discovered the SMBLoris vulnerability.

Besides EternalBlue, the NotPetya and Bad Rabbit ransomware outbreaks also utilized the EternalRomand exploit that Dillon has recently ported to target a more broader spectrum of Windows versions.

Dillon also included the following disclaimed with his ports, wanting people to know the code was created to help companies identify vulnerable machines through pen-testing and develop mitigation strategies.

> This software has been created purely for the purposes of academic research and for the development of effective defensive techniques, and is not intended to be used to attack systems except where explicitly authorized. Authors and

project maintainers are not responsible or liable for misuse of the software. Use responsibly.

ETERNALBLUE ETERNALCHAMPION ETERNALROMANCE ETERNALSYN

EXPLOIT NSA SHADOW BROKERS WINDOWS

SHARE TWEET

TAGGED: NEWS APPLE CYBERSECURITY IPHONE JAILBREAK IOS INFOSEC TECH NEWS INFORMATION SECURITY JAILBREAKING IBOOT