Security Newsletter

30 September 2019

Subscribe to this newsletter

Anonymous researcher drops vBulletin zero-day impacting tens of thousands of sites

An anonymous security researcher has published details about a zero-day in vBulletin. Despite being a commercial product, vBulletin is today's most popular web forum software package, with a larger market share than open-source solutions like phpBB, XenForo, Simple Machines Forum, MyBB, and others. According to W3Techs, around 0.1% of all internet sites run a vBulletin forum. The percentage looks small, but it actually impacts billions of internet users.

This is a critical vulnerability as it allows an attacker to execute any command on the site, which could allow them to download malware, reverse shells, or tamper with the site's code. After news broke about this vulnerability, Chaouki Bekrar, the CEO of the Zerodium exploit acquisition company, tweeted that his company has known about this exploit for three years and that many researchers have been selling the exploit for some time. So while this public disclosure may have increased the uptick of attacks using this vulnerability, it has most likely been secretly used for some time.

The vBulletin team has released a patch for this vulnerability, which is now tracked under the CVE-2019-16759. ZDNet has also confirmed with Bad Packets, BinaryEdge, and GeryNoise that hackers are now actively using this vulnerability to attack vulnerable forums.

Read More pm ZDNet

Even More on BleepingComputer

Hacker Releases 'Unpatchable' Jailbreak For All iOS Devices, iPhone 4s to iPhone X

An iOS hacker and cybersecurity researcher today publicly released what he claimed to be a "permanent unpatchable bootrom exploit," in other words, an epic jailbreak that works on all iOS devices ranging from iPhone 4s (A5 chip) to iPhone 8 and iPhone X (A11 chip). Since the bootrom exploits are hardware-level issues and can not be patched without a hardware revision, a simple software update can't address the newly released bootrom exploit.

Dubbed Checkm8, the exploit leverages unpatchable security weaknesses in Apple's Bootrom (SecureROM), the first significant code that runs on an iPhone while booting, which, if exploited, provides greater system-level access. The new exploit came exactly a month after Apple released an emergency patch for another critical jailbreak vulnerability that works on Apple devices including the iPhone XS, XS Max, and XR and the 2019 iPad Mini and iPad Air, running iOS 12.4 and iOS 12.2 or earlier.

It should be noted that the Checkm8 exploit itself is not a full jailbreak with Cydia, instead, is just an exploit which researchers and jailbreak community can use to develop a fully working jailbreak tool. The jailbreak only works on iPhones running Apple's A5 and A11 chipsets and does not work on the latest two chipsets, i.e., A12 and A13.

Read More on TheHackerNews

Magecart skimmers seen targeting routers for customer Wi-Fi networks

Threat researchers at IBM X-Force IRIS have spotted activity by a known group of criminal Web malware operators that appears to be targeting commercial layer 7 routers, the type typically associated with Wi-Fi networks that use "captive portals" to either charge for Internet access or require customers to sign in. In the past, Magecart attacks have focused on exploiting Web infrastructure components of victims' e-commerce sites.

The group, called "Magecart 5," is one of several factions of criminal groups originally associated with the Magecart "web-skimmer," a class of JavaScript-based payment card stealing malware that has been used in the past to target customers on e-commerce websites. Ticketmaster, British Airways, and NewEgg customers were just some of the victims in a rash of exploits by Magecart rings in 2018, and the malware operators have continued to be active in 2019. According to researchers, hundreds of thousands of merchant sites have been compromised through attacks on third-party services.

The researchers also found evidence that the group was making modifications to an open source mobile application library used to create touch "sliders" to allow users to swipe through galleries. "[Magecart 5] has likely infected this code, corrupting it at its source to ensure that every developer using the slider will end up serving the attackers' malicious code, leading to the compromise of user data of those using the finished product." That matches with Magecart 5's modus operandi of compromising third-party resources to get a broader effect, the researchers noted.

Read More on ArsTechnica

Even More on ZDNet

More #News

- 75% of execs cite phishing as the most significant security threat to businesses
- Investors accuse FedEx of lying, stock dumping after NotPetya attack
- YouTube 'influencers' get 2FA tokens phished
- 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day
- Microsoft Warns of a New Rare Fileless Malware Hijacking Windows Computers
- DoorDash Breach Exposes 4.9 Million Users' Personal Data
- Microsoft Explains Why Signed PowerShell Cmdlets May Run Slow
- Responding to email-based attacks takes over three hours, on average
- Researchers Disclose Another SIM Card Attack Possibly Impacting Millions
- Are you sure you wiped your hard drive properly?
- Outlook for Web Bans 38 More File Extensions in Email Attachments
- iOS 13 Bug Lets 3rd-Party Keyboards Gain 'Full Access' — Even When You Deny
- Microsoft to Extend Office 365 ATP Safe Links to Office Online
- WARP is here (sorry it took so long) - Wireguard based free VPN service
- Azure Sentinel, Microsoft's cloud-based SIEM, hits general availability
- Behind the scenes of a massively distributed credential stuffing attack

#Patch Time!

- Jira development and ticketing software hit by critical flaws
- Microsoft Releases Emergency Patches for IE 0-Day and Windows Defender Flaw
- Privilege escalation vulnerability patched in Forcepoint VPN for Windows
- Cisco Fixes Critical IOx Flaw Allowing Root Access to Guest OS
- VMware Patches Critical Harbor Vulnerability
- Apple users, patch now! The 'bug that got away' has been fixed
- Hackers are infecting WordPress sites via a defunct plug-in
- Update ColdFusion now! Emergency patch for critical flaws
- vBulletin Patches Vulnerability Exploited in the Wild

#Tech and #Tools

- How to bypass Android certificate pinning and intercept SSL traffic
- XSS cheat sheet - updated
- xip.io - Wildcard DNS for everyone
- CURRYFINGER - SNI & Host header spoofing utility
- 5 Easy Router Protection Techniques - includes Attack and Packet Analysis
- Sniffle: A Sniffer for Bluetooth 5
- Tool lists, Awesome...Security | Pentest | Malware analysis | Threat Intel
- How to Monitor GitHub for Secrets
- Staging over HTTPS and DNS simultaneously with Cobalt Strike and Shellter
- shhgit: Find GitHub secrets in real time
- A Pivot Cheatsheet for Pentesters

- Andromeda - Interactive Reverse Engineering Tool for Android Applications

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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