Security Newsletter

1 April 2019

Subscribe to this newsletter

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

The Taiwan-based tech giant ASUS is believed to have pushed the malware to hundreds of thousands of customers through its trusted automatic software update tool after attackers compromised the company's server and used it to push the malware to machines.

Researchers at cybersecurity firm Kaspersky Lab say that ASUS, one of the world's largest computer makers, was used to unwittingly install a malicious backdoor on thousands of its customers' computers last year after attackers compromised a server for the company's live software update tool. The malicious file was signed with legitimate ASUS digital certificates to make it appear to be an authentic software update from the company, Kaspersky Lab says.

"A small number of devices have been implanted with malicious code through a sophisticated attack on our Live Update servers in an attempt to target a very small and specific user group," says ASUS. The company also said that "only the version of Live Update used for notebooks has been affected," with all other devices not being affected by the supply chain attack. "customer service has been reaching out to affected users and providing assistance to ensure that the security risks are removed." Customers who discover that their machines have been affected are advised to "Immediately run a backup of your files and restore your operating system to factory settings. This will completely remove the malware from your computer."

Read More on MotherBoard

Even More on BleepingComputer

Magento's Latest Patches Should Be Applied Immediately

If your online e-commerce business is running over the Magento platform, you must pay attention to this information. Magento yesterday released new versions of its content management software to address a total of 37 newly-discovered security vulnerabilities. Owned by Adobe since mid-2018, Magento is one of the most popular content management system (CMS) platform that powers 28% of websites across the Internet with more than 250,000 merchants using the open source e-commerce platform.

Though most of the reported issues could only be exploited by authenticated users, one of the most severe flaws in Magento is an SQL Injection vulnerability which can be exploited by unauthenticated, remote attackers.

"Unauthenticated attacks, like the one seen in this particular SQL injection vulnerability, are very serious because they can be automated - making it easy for hackers to mount successful, widespread attacks against vulnerable websites," Montpas writes. "The number of active installs, the ease of exploitation and the effects of a successful attack are what makes this vulnerability particularly dangerous." The vulnerabilities are present within the open source and commercial versions of Magento. Magento advised that users should upgrade to versions 2.3.1 or 2.2.8.

Read More on BankInfoSecurity

Even More on TheHackerNews

More #News

- Man jailed for destroying former employer's data
- Unpatched Zero-Days in Microsoft Edge and IE Browsers Disclosed Publicly
- French gas stations robbed after forgetting to change gas pump PINs

- Huawei savaged by Brit code review board over poor dev practices
- Toyota Security Breach Exposes Personal Info of 3.1 Million Clients
- FireEye debuts Windows Commando VM as Linux Kali rival
- DragonEx exchange hacked, smoking ashes being raked over
- Security Nightmare: Users Fail to Wipe USB Drives
- Zero-Day TP-Link SR20 Router Vulnerability Disclosed by Google Dev
- Report deems Russia a pioneer in GPS spoofing attacks
- Facebook's Whitehat Settings lets bug-hunters dial back app security
- BoringTun, a userspace WireGuard implementation in Rust
- Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers
- MAC Addresses Targeted by the ASUS Supply Chain Attack Now Available
- World Backup Day: Is your data in safe hands?
- 90% of large tech companies vulnerable to email spoofing

#Patch Time!

- VMware Fixes Critical Vulnerabilities in ESXi, Workstation and Fusion
- Cisco Improperly Patched Exploited Router Vulnerabilities
- Apple Patches Vulnerabilities in iOS, macOS, Safari
- Nvidia patches code execution vulnerability in GeForce Experience
- Magento 2.3.1, 2.2.8 and 2.1.17 Security Update

#Tech and #Tools

- PoC || GTFO 0x19
- Disclosing a directory traversal vulnerability in Kubernetes copy – CVE-2019-1002101
- Endlessh: an SSH Tarpit
- A Pentester's Guide – Part 1 (OSINT – Passive Recon and Discovery of Assets)
- Osmedeus – Fully Automated Offensive Security Tool for Reconnaissance & Vulnerability Scanning
- commando-vm
- Operation ShadowHammer
- Over 9,000 Cisco RV320/RV325 routers are vulnerable to CVE-2019-1653
- In-depth analysis of MageCart skimming scripts
- mkYARA – Writing YARA rules for the lazy analyst
- Magento 2.2.0 <= 2.3.0 Unauthenticated SQLi
- Owning the Network with BadUSB
- ICMP-REACHABLE: Bypassing firewalls with ICMP error messages

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