Apple Patches 21 Vulnerabilities in WebKit

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/_w4lwC9XsPg/apple-patches-21-vulnerabilities-webkit

---

WhatsApp Vulnerability Exploited to Spy on Users

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/kqvB5h2NhdY/facebook-patches-whatsapp-flaw-exploited-spy-users

---

Microsoft SharePoint Vulnerability Exploited in the Wild

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tQEzQHO2uxc/microsoft-sharepoint-vulnerability-exploited-wild

Over 100 Flaws Expose Buildings to Hacker Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/H-L0CD7muK4/over-100-flaws-expose-buildings-hacker-attacks

---

Open source bug poses threat to sites running multiple CMSes

reader comments

33 with 24 posters participating

Share this story

Websites running the Drupal, Joomla, or Typo3 content-management systems are vulnerable to attacks that could possibly execute malicious code until administrators install just-released patches, developers and security researchers warned.

The vulnerability resides in the PharStreamWrapper, a PHP

component developed and open-sourced by CMS maker Typo3. Indexed as CVE-2019-11831, the flaw stems from a path-traversal bug that allows hackers to swap a site's legitimate phar archive with a malicious one. A phar archive is used to distribute a complete PHP application or library in a single file, in much the way a Java archive file bundles many Java files into a single file.

In an advisory published Wednesday, Drupal developers rated the severity of the vulnerability affecting their CMS as moderately critical. That's well below the highly critical rating of a recent Drupal vulnerability and earlier remote-execution flaws that took on the name "Drupalgeddon." Still, the vulnerability represents enough of a risk that administrators should patch it as soon as possible.

"The nature of the [pharStreemWarapper] vulnerability makes it context dependent," Daniel le Gall, a researcher who discovered the vulnerability, told Ars. "I found this vulnerability on Drupal, and that's the only platform where I assessed the severity. I'm currently talking with Drupal to make it 'critical' instead of 'moderately critical,' but the final decision is in their hands."

A researcher at SCRT SA in Switzerland, le Gall said his own calculus using Drupal's published severity rating method led him to the determination the vulnerability should be rated critical. Still, he agreed that CVE-2019-11831 was well below the threshold of previous Drupal bugs, which could be exploited by unprivileged end users visiting a vulnerable site.

"For a default Drupal [site] without plugins, it requires [the site] to have a user with the 'Administer theme' right, which is a high prerequisite," he said. That means that an attacker would have to have limited administrator privileges, such as those given to marketing people or graphic designers.

“However, some community modules might be vulnerable because of this flaw in the Drupal Core,” he added. “Once these privileges are obtained, the flaw is pretty easy to exploit, however, and effectively leads to remote code execution.”

Joomla developers, meanwhile, issued their own advisory on Wednesday that rated the severity low. Typo3 developers didn’t provide a severity rating for their own CMS.

Sites that run:

- Drupal 8.7 should update to 8.7.1
- 8.6 or earlier should update to 8.6.16
- 7 should update to 7.67

On Joomla, the flaw affects versions 3.9.3 through 3.9.5. The fix is available in 3.9.6.

Typo3 CMS users should either upgrade to PharStreamWapper versions v3.1.1 and v2.1.1 manually or ensure Composer dependencies are raised to those versions.

https://arstechnica.com/?p=1502725

Phar Vulnerabilities Patched in Drupal, TYPO3

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/8sMpg59DTo8/phar-vulnerabilities-patched-drupal-typo3

WordPress 5.2 Brings New Security Features

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/SXuYWupwKpU/wordpress-52-brings-new-security-features

---

Jenkins Vulnerability Exploited to Deliver ‘Kerberods’ Malware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/EB6Bu8vge30/jenkins-vulnerability-exploited-deliver-kerberods-malware

---

Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak

Enlarge / The National Security Agency headquarters in Fort Meade, Maryland.

reader comments

33 with 21 posters participating

Share this story

On of the most significant events in computer security happened in April 2017, when a still-unidentified group calling itself the Shadow Brokers published a trove of the National Security Agency's most coveted hacking tools. The leak and the subsequent repurposing of the exploits in the WannaCry and NotPetya worms that shut down computers worldwide made the theft arguably one of the NSA's biggest operational mistakes ever.

On Monday, security firm Symantec reported that two of those advanced hacking tools were used against a host of targets starting in March 2016, fourteen months prior to the Shadow Brokers leak. An advanced persistent threat hacking group that Symantec has been tracking since 2010 somehow got access to a variant of the NSA-developed "DoublePulsar" backdoor and one of the Windows exploits the NSA used to remotely install it on targeted computers.

Killing NOBUS

The revelation that the powerful NSA tools were being repurposed much earlier than previously thought is sure to touch off a new round of criticism about the agency's inability to secure its arsenal.

"This definitely should bring additional criticism of the ability to protect their tools," Jake Williams, a former NSA hacker who is now a cofounder of Rendition Infosec, told Ars. "If they didn't lose the tools from a direct compromise, then the exploits were intercepted in transit or they were independently discovered. All of this completely kills the NOBUS argument."

“NOBUS” is shorthand for nobody but us, a mantra NSA officials use to justify their practice of privately stockpiling certain exploits, rather than reporting the underlying vulnerabilities so they can be fixed.

Symantec researchers said they didn’t know how the hacking group—variously known as Buckeye, APT3, Gothic Panda, UPS Team, and TG-0110—obtained the tools. The researchers said the limited number of tools used suggested the hackers’ access wasn’t as broad as the access enjoyed by the Shadow Brokers. The researchers speculated that the hackers may have reverse engineered technical “artifacts” they captured from attacks the NSA carried out on it own targets. Other less likely possibilities, Symantec said, were Buckeye stealing the tools from an unsecured or poorly secured NSA server, or a rogue NSA group member or associate leaking the tools to Buckeye.

The attack used to install Buckeye’s DoublePulsar variant exploited a Windows vulnerability indexed as CVE-2017-0143. It was one of several Windows flaws exploited in Shadow Broker-leaked NSA tools with names like “Eternal Romance” and “Eternal Synergy.” Microsoft patched the vulnerability in March 2017 after being tipped off by NSA officials that the exploits were likely to be published soon.

Symantec’s report means that by the time the NSA reported the vulnerabilities to Microsoft, they had already been exploited in the wild for months.

“The fact that another group (besides NSA) were able to successfully exploit the Eternal series of vulnerabilities…is very impressive,” Williams said. “It speaks to their technical abilities and resourcing. Even if they stole the vulnerabilities while they were being used on the network, that’s not enough to recreate reliable exploitation without tons of extra research.”

Tale of two exploits

Security protections built into modern versions of Windows required two separate vulnerabilities be exploited to successfully install DoublePulsar. Both the NSA and Buckeye started by using CVE-2017-0143 to corrupt Windows memory. From there, attackers needed to exploit a separate vulnerability that would divulge the memory layout of the targeted computer. Buckeye relied on a different information-disclosure vulnerability than the NSA's Eternal attacks used. The vulnerability used by Buckeye, CVE-2019-0703, received a patch in March, six months after Symantec privately reported it to Microsoft.

Symantec said the earliest known instance of Buckeye using the NSA variants came on March 31, 2016 in an attack on a target in Hong Kong. It came in a custom-designed trojan dubbed "Bemstour" that installed DoublePulsar, which runs only in memory. From there, DoublePulsar installed a secondary payload that gave the attackers persistent access to the computer, even if it was rebooted and DoublePulsar was no longer running. An hour after the Hong Kong attack, Buckeye used Bemstour against an educational institution in Belgium.

Six months later—sometime in September, 2016—Buckeye unleashed a significantly updated variant of Bemstour on an educational institution in Hong Kong. One improvement: unlike the original Bemstour, which ran only on 32-bit hardware, the updated version ran on 64-bit systems as well. Another advance in the updated Bemstour was its ability to execute arbitrary shell commands on the infected computer. This allowed the malware to deliver custom payloads on 64-bit infected computers. The attackers typically used the capability to create new user accounts.

Bemstour was used again in June 2017 against a target in Luxembourg. From June to September of that year Bemstour

infected targets in the Philippines and Vietnam. Development of the trojan continued into this year, with the most recent sample having a compilation date of March 23, 11 days after Microsoft patched the CVE-2019-0703 zero-day.

Symantec researchers were surprised to see Bemstour being actively used for so long. Previously, the researchers believed that APT3 had disbanded following the November 2017 indictment of three Chinese nationals on hacking charges. While the indictment didn't identify the group the defendants allegedly worked for, some of the tools prosecutors identified implicated APT3.

Monday's report said Bemstour's use following the apparent disappearance of Buckeye remained a mystery.

"It may suggest that Buckeye retooled following its exposure in 2017, abandoning all tools publicly associated with the group," company researchers wrote. "However, aside from the continued use of the tools, Symantec has found no other evidence suggesting Buckeye has retooled. Another possibility is that Buckeye passed on some of its tools to an associated group."

https://arstechnica.com/?p=1501137

PrinterLogic Vulnerability Allows Remote Code Execution

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/18vgv1-SFQY/printerlogic-vulnerability-allows-remote-code-execution