Potent Firefox 0-day used to install undetected backdoors on Macs

Enlarge / The fox animoji.

reader comments

22 with 19 posters participating

Share this story

Hackers exploited a pair of potent zero-day vulnerabilities in Firefox to infect Mac users with a largely undetected backdoor, according to accounts pieced together from multiple people.

Mozilla released an update on Tuesday that fixed a code-execution vulnerability in a JavaScript programming method known as Array.pop. On Thursday, Mozilla issued a second patch fixing a privilege-escalation flaw that allowed code to break out of a security sandbox that Firefox uses to prevent untrusted content from interacting with sensitive parts of a computer operating system. Interestingly, a researcher at Google's Project Zero had privately reported the code-execution flaw to Mozilla in mid April.

On Monday, as Mozilla was readying a fix for the array.pop flaw, unknown hackers deployed an attack that combined working exploits for both vulnerabilities. The hackers then used the attack against employees of Coinbase, according to Philip Martin, chief information security officer for the digital currency exchange.

> *2/ We walked back the entire attack, recovered and reported the 0-day to firefox, pulled apart the malware and infra used in the attack and are working with various orgs to continue burning down attacker infrastructure and digging into the attacker involved.*
>
> *— Philip Martin (@SecurityGuyPhil) June 19, 2019*

"We've seen no evidence of exploitation targeting customers," Martin added. "We were not the only crypto org targeted in this campaign. We are working to notify other orgs we believe were also targeted." Martin also published cryptographic hashes of code used in the attack, along with IP addresses the code contacted.

The plot thickens

On Thursday, macOS security expert Patrick Wardle published an analysis of Mac malware that came from someone who claimed it infected his fully up-to-date Mac through a zero-day vulnerability in Firefox. The person claimed to have been "involved with a cryptocurrency exchange until fairly recently." The hash of the malware matched one of the hashes provided by Martin.

Among the things Wardle noticed early on was that the VirusTotal service showed that the malware was detected by only one of what at the time was 53 available malware detectors (at the time this Ars post went live, five out of 57 engines flagged it). That was strange, because XProtect, the barebones malware detector built into macOS, had been detecting the NetWire sample since 2016. It's surprising malware detectors hadn't obtained a detection signature from Apple. Wardle also noticed that the malware sample wasn't digitally signed by its developer.

Normally, an app that's blacklisted by XProtect and unsigned

should have posed no threat to most Mac users, since the software would have been blocked by default by both the built-in malware detector and Gatekeeper. This is a protection that, by default, requires apps to be signed by a known developer before they can be installed. But because NetWire was installed through a privileged process tied to Firefox, the exploit was able to bypass both protections. The reason: the file lacked a "quarantine" bit that's only set when a user downloads the file from the Internet.

"In a nutshell, since XProtect and Gatekeeper only scan files that have the quarantine bit set, no, they would not have protected the user," Wardle, who is chief research officer at Digita Security, told Ars. "Why? When an exploit downloads a file (versus the user), that bit wouldn't be set." As a result, he added: "There would be no visual indication of an infection—unless the user went digging."

By digging, Wardle means manually inspecting a Mac to see what apps have permission to install themselves when the OS is booting. This can be done using security tools such as KnockKnock or BlockBlock, which are freely available from Wardle. It turns out, the Netwire sample used not one, but two relatively primitive methods to maintain persistence on a Mac.

Patrick Wardle
Wardle said he believes that Apple is in the process of updating XProtect and Gatekeeper so they scan all files, not just those with a quarantine bit. He said the change may be introduced in macOS 10.15.

The second hash Martin provided corresponds to a different piece of Mac software that, at the time this post went live, was undetected by all covered products. Wardle has yet to analyze it, so the threat it poses wasn’t immediately clear. Both he and independent reverse-engineer Vitali Kremez told Ars there appears to be a separate piece of malware that has backdoor and remote trojan properties. This post will be updated as more information becomes available.

Gone phishin’

Wardle also published an email the person who contacted him said contained a link to the drive-by site that exploited the

Firefox zero-day. Here's the slightly redacted text:

> *Dear XXX,*
>
> *My name is Neil Morris. I'm one of the Adams Prize Organizers.*
>
> *Each year, we update the team of independent specialists who could assess the quality of the competing projects: http://people.ds.cam.ac.uk/nm603/awards/Adams_Prize*
>
> *Our colleagues have recommended you as an experienced specialist in this field.*
>
> *We need your assistance in evaluating several projects for Adams Prize.*
>
> *Looking forward to receiving your reply.*
>
> *Best regards,*
> *Neil Morris*

By the time Wardle visited the site, it was returning a 404 error indicating it was no longer available.

A Windows component?

While both of the hashes provided by Martin applied to apps that run only on macOS, one of the command and control servers has also been known to control a Windows backdoor with characteristics that are similar to NetWire, according to this analysis from Kremez, the independent reverse engineer. The same analysis shows links to two other in-the-wild attacks, one exploiting a nasty vulnerability in the WinRAR Windows file compression program, and the other against a Microsoft Word zero-day in 2017.

"I do not have direct evidence [Windows users] were targeted as a result of this exploit," Kremez told Ars referring to the

one against Firefox. “The previous cases suggest they were—but it is unconfirmed in this case as the evidence is scarce.”

https://arstechnica.com/?p=1525253

Firefox Zero-Day Exploited to Deliver Malware to Cryptocurrency Exchanges

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/A7B5smE_PGM/firefox-zero-day-exploited-deliver-malware-cryptocurrency-exchanges

---

Critical Vulnerabilities Patched in Cisco SD-WAN, DNA Center Products

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/qKxiJqY61ew/critical-vulnerabilities-patched-cisco-sd-wan-dna-center-products

Oracle issues emergency update to patch actively exploited WebLogic flaw

Enlarge / Security team KnownSec404 proof-of-concept image, showing an instance of Windows Calculator being run on the remote WebLogic server.

reader comments

17 with 10 posters participating, including story author

Share this story

Oracle on Tuesday published an out-of-band update patching a critical code-execution vulnerability in its WebLogic server after researchers warned that the flaw was being actively exploited in the wild.

The vulnerability, tracked as CVE-2019-2729, allows an attacker to run malicious code on the WebLogic server without any need for authentication. That capability earned the vulnerability a Common Vulnerability Scoring System score of 9.8 out of 10. The vulnerability is a deserialization attack targeting two Web applications that WebLogic appears to expose to the Internet by default—wls9_async_response and wls-wsat.war.

The flaw in Oracle's WebLogic Java application servers came to light as a zero-day four days ago when it was reported by security firm KnownSec404.

This isn’t the first, or even second, deserialization attack that has been used to target these services. The wls-wsat component was successfully exploited in a similar fashion in 2017, and KnownSec404 reported another one in April. The 2017 vulnerability was largely used to install bitcoin miners; April’s vulnerability was exploited in cryptojacking and ransomware campaigns. Oracle’s current out-of-band patch and advisory notice has not officially acknowledged the active exploitation of CVE-2019-2729, but it does mark the vulnerability as high risk and advises customers to apply the out-of-band patch as soon as possible.

According to Johannes Ullrich of the SANS Technology Institute, Oracle has been patching each of these series of deserialization vulnerabilities by individually blacklisting the deserialization of very specific classes as exploits are published. This implies the likelihood of an ongoing cat-and-mouse game in which attackers who understand the service well continue to find and exploit a pool of available vulnerabilities as needed and sparingly.

KnownSec404 recommends mitigating these vulnerabilities ahead of the patch by either disabling the affected Asynchronous Request-Response and Web Service Atomic Transactions applications entirely, or by controlling access to them by network policy. Considering the frequency and active exploitation of vulnerabilities on these services, it’s probably an excellent idea to at least limit access to them as narrowly as possible. User posts on StackOverflow and Oracle’s support site make it clear that WebLogic users are disabling the two affected apps entirely, making sweeping statements to the effect of “you don’t need them anyway.” But without fully understanding the scope and utility of components installed by default, administrators should be very careful and extensively test any such modifications.

https://arstechnica.com/?p=1524451

Oracle Patches Another Remote Code Execution Flaw in WebLogic

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5gk6yWsanKk/oracle-patches-another-remote-code-execution-flaw-weblogic

---

Firefox Zero-Day Vulnerability Exploited in Targeted Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/p26tPTHWeR0/firefox-zero-day-vulnerability-exploited-targeted-attacks

---

Facebook Open Sources CTF

2019 Challenges

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ijLXYdk308A/facebook-open-sources-ctf-2019-challenges

---

Serious Vulnerabilities in Linux Kernel Allow Remote DoS Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/jd8VZUJJ0Cg/serious-vulnerabilities-linux-kernel-allow-remote-dos-attacks

---

DHS Issues Alert for Windows ‘BlueKeep’ Vulnerability

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5KzgUANczTE/dhs-issues-alert-windows-bluekeep-vulnerability

---

Vulnerabilities Expose BD Infusion Therapy Devices to Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/N8WmetR3Hx8/vulnerabilities-expose-bd-infusion-therapy-devices-attacks