

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own

Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own

By
Sergiu Gatlan
(<https://www.bleepingcomputer.com/author/sergiu-gatlan/>)

May 24, 2022

05:31 PM

0



Mozilla has released security updates for multiple products to address zero-day vulnerabilities exploited during the Pwn2Own Vancouver 2022 hacking contest.

If exploited, the two critical flaws can let attackers gain JavaScript code execution on mobile and desktop devices running vulnerable versions of Firefox, Firefox ESR, Firefox for Android, and Thunderbird.

The zero-days have been fixed in Firefox 100.0.2, Firefox ESR 91.9.1, Firefox for Android 100.3, and Thunderbird 91.9.1.

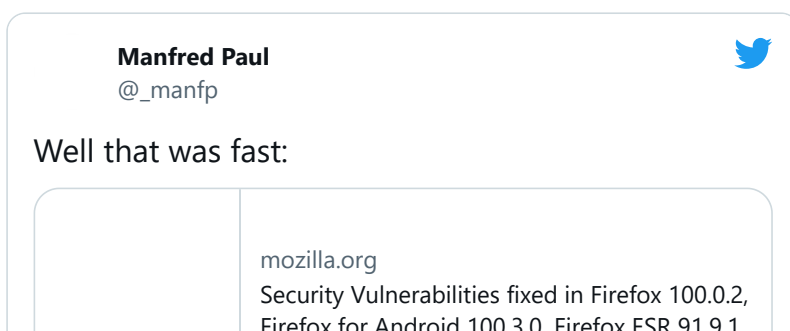


Manfred Paul (@_manfp (https://twitter.com/_manfp)) earned \$100,000 and 10 Master of Pwn points after demoing prototype pollution and improper input validation bugs on the first day of Pwn2Own (<https://www.bleepingcomputer.com/news/security/microsoft-teams-windows-11-hacked-on-first-day-of-pwn2own/>).

The first vulnerability is a prototype pollution in Top-Level Await implementation (tracked as CVE-2022-1802 (<https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/#CVE-2022-1802>)) that can let an attacker corrupt the methods of an Array object in JavaScript using prototype pollution to achieve JavaScript code execution in a privileged context.

The second one (CVE-2022-1529 (<https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/#CVE-2022-1529>)) allows attackers to abuse Java object indexing improper input validation in prototype pollution injection attacks.

"An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process," Mozilla explained (<https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/#CVE-2022-1529>).



The Cybersecurity and Infrastructure Security Agency (CISA) also encouraged (<https://www.cisa.gov/uscert/ncas/current-activity/2022/05/23/mozilla-releases-security-products-multiple-firefox-products>) admins and users on Monday to patch these security flaws, given that threat actors could exploit them to "take control of an affected system."

Mozilla patched these vulnerabilities two days after they were exploited and reported at the Pwn2Own hacking contest by Manfred Paul.

However, vendors don't usually hurry to release patches after Pwn2Own since they have 90 days to push security fixes until Trend Micro's Zero Day Initiative publicly discloses them.

Pwn2Own 2022 Vancouver ended on May 20 after 17 competitors earned \$1,155,000 (<https://www.zerodayinitiative.com/blog/2022/5/18/pwn2own-vancouver-2022-the-results#:~:text=Trend%20Micro%20and%20ZDI%20awarding%20%241%2C155%2C000>) for zero-day exploits and exploit chains demonstrated over three days after 21 attempts.

Security researchers also earned \$400,000 for 26 zero-day exploits (<https://www.bleepingcomputer.com/news/security/hackers-earn-400k-for-zero-day-ics-exploits-demoed-at-pwn2own/>) targeting ICS and SCADA products demoed between April 19 and April 21 during the 2022 Pwn2Own Miami contest.