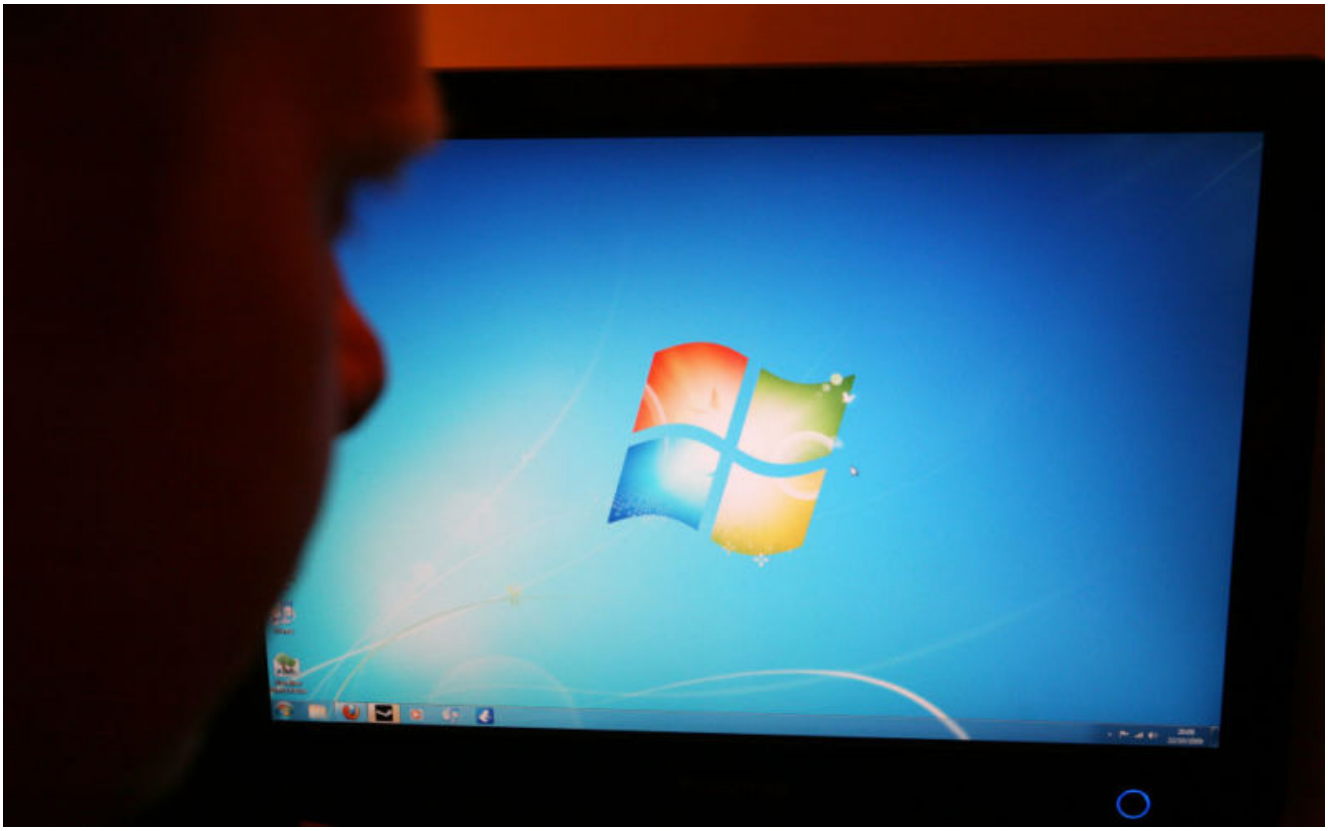
Microsoft patches 3 Windows 0days under active exploit



Enlarge / A man looks at the home screen for the “new” Windows 7 platform when it was launched in October 2009. Microsoft has ended support, but the OS lives on.

reader comments

7 with 6 posters participating

Share this story

Microsoft has patched three actively exploited vulnerabilities that allow attackers to execute malicious code or elevate system privileges on devices that run Windows.

Two of the security flaws—tracked as CVE-2020-1020 and CVE-2020-0938—reside in the Adobe Type Manager Library, a Windows DLL file that a wide variety of apps use to manage and render fonts available from Adobe Systems. On supported

operating systems other than Windows 10, attackers who successfully exploit the vulnerabilities can remotely execute code. On Windows 10, attackers can run code inside an AppContainer sandbox. The measure limits the system privileges malicious code has, but even then, attackers can use it to create accounts with full user rights, install programs, and view, change, or delete data.

Attackers can exploit the flaws by convincing a target to open a booby-trapped document or viewing it in the Windows preview pane. Tuesday's advisories said that Microsoft is "aware of limited, targeted attacks that attempt to leverage" both vulnerabilities. Microsoft revealed last month that one of the bugs was being exploited in limited attacks against Windows 7 machines.

While installing the newly available patches is the best way to protect vulnerable systems, temporary workarounds for those who need to buy more time include:

- Disabling the Preview Pane and Details Pane in Windows Explorer
- Disabling the WebClient service
- Rename ATMFD.DLL (on Windows 10 systems that have a file by that name), or alternatively, disable the file from the registry

These are the same mitigations that Microsoft recommended in its March advisory. Once the patches are installed, users can roll back the mitigations.

The last zeroday exploit targets CVE-2020-1027, an elevation of privilege flaw in the way that the Windows kernel handles objects in memory. Attackers who already have limited system rights on a vulnerable machine can use the exploit to execute malicious code. To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.

Microsoft didn’t provide any details about the attacks that are underway against the latter two flaws.

Threat analysis group gets credit

The software maker credited discovery of the zero-day exploits to Google’s threat analysis group, which tracks government-backed hack attacks against the company’s users.

Google’s threat analysis group reported the attacks against the Adobe Type Manager flaws on March 23 and, per the company’s disclosure policy for actively exploited bugs, gave Microsoft seven days to fix or disclose the flaw. Google later gave Microsoft an extension to accommodate work slowdowns caused by the novel coronavirus pandemic. Group members plan to issue a report that details the Adobe flaws in the next month or so. It’s not clear when the threat analysis group will provide details about the other two vulnerabilities.

Typically, Windows devices in home and smaller-office settings receive patches automatically within 24 hours. It’s always a good idea to make sure updates are installed within that time frame. Administrators in larger organizations face the sometimes-difficult task of testing patches before deploying them to ensure they’re compatible with systems already in place. That task is likely to be harder this month, with the work disruptions caused by COVID-19 infections sweeping the globe.

Post updated to correct the number of 0days. It’s three.

https://arstechnica.com/?p=1668426