Adobe Plugs Critical Security Holes in Illustrator, After Effects Software

Software maker Adobe on Tuesday released security fixes for at least a half dozen vulnerabilities that expose Windows and macOS users to malicious hacker attacks.

The Mountain View, Calif. company warned that the security problems exist on three of its most popular software products – Photoshop, Illustrator and After Effects.

According to Adobe's security bulletins, the Illustrator and After Effects patches carry critical-severity ratings because of the risk of code execution attacks.

The company said the Adobe Illustrator vulnerability, tracked as CVE-2022-23187, is a buffer overflow issue that leads to arbitrary code execution. The bug is present for both Windows and macOS users on Illustrator 26.0.3 and earlier versions.

A second critical bulletin was released to cover at least four documented Adobe After Effects vulnerabilities that expose Windows and macOS users to code execution attacks.

"This update addresses critical security vulnerabilities. Successful exploitation could lead to arbitrary code execution in the context of the current user," Adobe said in a bulletin that documents stack-based buffer overflows with serious implications.

Adobe tracks the After Effects bugs as CVE-2022-24094, CVE-2022-24095, CVE-2022-24096, and CVE-2022-24097.

The company also shipped a third bulletin to cover an important-severity flaw in its flagship Adobe Photoshop software.

The Photoshop vulnerability (CVE-2022-24090) affects both Windows and macOS users and Adobe warns that successful exploitation could lead to memory leak in the context of the current user.

Adobe said it was not aware of any exploits in the wild for any of the flaws patched this month.

Adobe's patches follow the release of patches from Apple to cover an already exploited WebKit zero-day affecting its iOS, iPadOS and macOS platforms.

The WebKit flaw, tracked as CVE-2023-23529, is described as a type confusion issue that can be exploited for arbitrary code execution by getting the targeted user to access a malicious website.

Related: Apple Patches Actively Exploited WebKit Zero-Day Vulnerability

Related: Microsoft Patch Tuesday: 97 Windows Vulns, 1 Exploited Zero-Day

Related: Zoom Patches High Risk Flaws on Windows, MacOS Platforms

Related: Microsoft Warns of Under-Attack Windows Kernel Flaw

Adobe Plugs Critical Security Holes in Illustrator, After Effects Software