

CISA Adds Chrome, macOS Bugs to Known Exploited Vulnerabilities Catalog

The US Cybersecurity and Infrastructure Security Agency (CISA) has added two flaws to its known exploited vulnerabilities (KEV) catalog: a Chrome bug patched last week and a macOS bug exploited by the DazzleSpy malware.

The Chrome vulnerability, tracked as CVE-2023-2033, was patched by Google on Friday with a Chrome 112 update. The flaw has been described as a type confusion issue affecting the V8 JavaScript engine.

Google has not shared any information about the attacks exploiting CVE-2023-2033. However, the issue was reported by a member of the company's Threat Analysis Group, which often finds vulnerabilities exploited by commercial spyware vendors.

The second vulnerability, CVE-2019-8526, is a privilege escalation issue affecting Apple's macOS operating system. A patch was released in March 2019 and the details of the flaw were made public a few months later by the researcher who reported it to the tech giant.

CVE-2019-8526, also known as KeySteal, affects macOS versions prior to 10.14.4 and it can be exploited to access passwords inside the Keychain without any warning to the user.

Cybersecurity firm ESET warned about exploitation of CVE-2019-8526 in January 2022, when it released a report on a piece of macOS malware dubbed DazzleSpy. The malware,

described as a full-featured backdoor that allows attackers to control the compromised device and steal data, was discovered during the analysis of an attack launched by a state-sponsored threat group against pro-democracy individuals in Hong Kong.

It's worth noting that Apple's advisory does not say anything about CVE-2019-8526 being exploited in attacks.

It's unclear if CISA has become aware of additional attacks exploiting CVE-2019-8526 or if it added the vulnerability to the KEV catalog due to the DazzleSpy attacks. Considering that the KeySteal exploit has been publicly available for years, it's possible that other threat actors have added it to their arsenal.

CISA has instructed federal agencies to patch CVE-2019-8526 and CVE-2023-2033 until May 8. Other organizations should also ensure that the vulnerabilities included in the KEV catalog are patched.

Related: Google, CISA Warn of Android Flaw After Reports of Chinese App Zero-Day Exploitation

Related: CISA Warns of Plex Vulnerability Linked to LastPass Hack

Related: Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA 'Must Patch' List

CISA Adds Chrome, macOS Bugs to Known Exploited Vulnerabilities Catalog