CISA adds 8 vulnerabilities to list of actively exploited bugs

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** January 31, 2022 01:18 PM **0**

US Cybersecurity & Infrastructure Security Agency (CISA) has added

The goal of publishing these vulnerabilities is to raise awareness and remind federal organizations of their obligation to apply security updates by a specified strict deadline.

execute commands remotely.

The eight flaws added by CISA last week (http://www.cisa.gov/uscert/ncas/current-activity/2022/01/28/cisa-adds-eight-known-exploited-vulnerabilities-catalog) are listed below:

CVE ID	Description	Patch Deadline
CVE-2022-22587	Apple IOMobileFrameBuffer Memory Corruption Vulnerability	2/11/2022
CVE-2021-20038	SonicWall SMA 100 Appliances Stack-Based Buffer Overflow Vulnerability	2/11/2022
CVE-2014-7169	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability	7/28/2022
CVE-2014-6271	GNU Bourne-Again Shell (Bash) Arbitrary Code Execution Vulnerability	7/28/2022
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service (BITS) Improper Privilege Management Vulnerability	7/28/2022
CVE-2014-1776	Microsoft Internet Explorer Use-After-Free Vulnerability	7/28/2022

CVE-2017-5689	Intel Active Management Technology (AMT), Small Business Technology (SBT), and Standard Manageability Privilege Escalation	7/28/2022

affecting iOS, iPadOS, and macOS "Monterey."

Apple released a security update (https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-exploited-to-hack-macos-ios-devices/) to fix the zero-day last Wednesday, warning that it is actively exploited in attacks. Due to the potential impact of this vulnerability on devices with wide circulation, CISA has given federal agencies until February 11, 2022, to apply the security updates.

CISA also added the **CVE-2021-20038** vulnerability affecting SonicWall SMA 100 Appliances after it was discovered that threat actors were actively scanning for and attempting to exploit the vulnerability (https://www.bleepingcomputer.com/news/security/attackers-now-actively-targeting-critical-sonicwall-rce-bug/). As a result, CISA also requires agencies to patch this bug by February 11, 2022.

Of the older flaws, CVE-2013-6271 holds special significance for being a reliable long-term intrusion channel for adversaries.

in the context of global-scale sophisticated DNS hijacking attacks.

It appears that many system administrators still find it practically challenging to apply the fixing updates after almost eight years since they were first made publicly available.

With the addition of these eight vulnerabilities, there is now a total of 351 exploited vulnerabilities listed in CISA's Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog).

Related Articles:

Apple fixes new zero-day exploited to hack macOS, iOS devices (https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-exploited-to-hack-macos-ios-devices/)

CISA adds 17 vulnerabilities to list of bugs exploited in attacks (https://www.bleepingcomputer.com/news/security/cisa-adds-17-vulnerabilities-to-list-of-bugs-exploited-in-attacks/)

CISA alerts federal agencies of ancient bugs still being exploited (https://www.bleepingcomputer.com/news/security/cisa-alerts-federal-agencies-of-ancient-bugs-still-being-exploited/)

Microsoft: powerdir bug gives access to protected macOS user data (https://www.bleepingcomputer.com/news/microsoft/microsoft-powerdir-bug-gives-access-to-protected-macos-user-data/)

Apple iOS vulnerable to HomeKit 'doorLock' denial of service bug (https://www.bleepingcomputer.com/news/security/apple-ios-vulnerable-to-homekit-doorlock-denial-of-service-bug/)