CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

*CYBER ADVISORY*

18 October 2024

# Windows October Patch – Two Known Exploited Vulnerabilities

CVE-2024-43572 | CVE-2024-43573 | Windows | CISA KEV

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical vulnerabilities under active exploitation known as CVE-2024-43572 and CVE-2024-43573.[1] A vulnerability in Microsoft Management Console (MMC) allows an attacker to exploit CVE-2024-43572 by deploying a malicious MMC Snap-in file resulting in remote code execution.[2][3] A flaw in Microsoft HTML (MSHTML) allows an attacker to exploit CVE-2024-43573 by spoofing web resources through invoking Internet Explorer 11 resulting in remote code execution.[4]

The Cal-CSIC recommends immediately updating to the latest Microsoft October Security Updates.

For further information on applying updates please refer to Microsoft October Release Notes.

## Organization, Source, Reference, and Dissemination Information

| | |
|---|---|
| **Organization Description** | California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state. |
| **Customer Feedback** | If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov. |
| **Source Summary Statement** | This report was compiled from a variety of sources, predominately open-source reporting. |

**WARNING:** This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

| | |
|---|---|
| **Handling Caveats** | **Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |
| **Information Needs** | *HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5* |

[1] Cybersecurity and Infrastructure Security Agency. (2024, October 8). *CISA adds three known exploited vulnerabilities to catalog*. CISA. “https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-adds-three-known-exploited-vulnerabilities-catalog”; Date Accessed 14 October 2024.

[2] Broadcom. (2024). *CVE-2024-43572: Microsoft Windows Management Console RCE vulnerability*. Broadcom. “https://www.broadcom.com/support/security-center/protection-bulletin/cve-2024-43572-microsoft-windows-management-console-rce-vulnerability”; Date Accessed 14 October 2024.

[3] Elastic. (2024). *GrimResource: An advanced exploitation technique*. Elastic Security Labs. “https://www.elastic.co/security-labs/grimresource”; Date Accessed 14 October 2024.

[4] The Hacker News. (2024, October). *Microsoft issues security update fixing critical RCE vulnerabilities*. The Hacker News. “https://thehackernews.com/2024/10/microsoft-issues-security-update-fixing.html”; Date Accessed 14 October 2024.

CAL-CSIC-202410-007

**WARNING:** This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

2