



INFORMATIONAL

HC3: Monthly Cybersecurity Vulnerability Bulletin



TLP:WHITE

Jan 17, 2025

Health Sector Cybersecurity Coordination Center (HC3) has shared a report regarding vulnerabilities impacting information systems relevant to the health sector for December 2024. This includes the monthly Patch Tuesday vulnerabilities released by several vendors on the second Tuesday of each month, along with mitigation steps and/or patches. Vulnerabilities for December 2024 are from Microsoft, Google/Android, Apple, Mozilla, Cisco, SAP, Adobe, Fortinet, Ivanti, VMware and Atlassian.

Health-ISAC recommends applying the latest patches for instances affected by the vulnerabilities, with special consideration given to each vulnerability criticality category against the organization's risk management posture. As always, accountability, proper inventory management, device hygiene, and asset tracking are imperative to an effective patch management program.

For additional information, please see the attached report for details or search the Doc Library under Government > HC3 > HC3 Monthly Cybersecurity Vulnerability Bulletin

Report Source(s)

HC3

Release Date

Jan 18, 2025 (UTC)

Alert ID 53827c6d

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

[View Alert](#)

Share Feedback

was this helpful?  | 

Tags HC3

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.

Powered by [Cyware](#)