VULNERABILITY BULLETINS

Ivanti Patches Four Critical Flaws Affecting Several Products

TLP:WHITE

Feb 12, 2025

On February 11, 2025, Ivanti issued security updates to fix several vulnerabilities affecting Connect Secure (ICS), Policy Secure (IPS), and Cloud Services Application (CSA). The four most critical flaws in the batch have CVSS scores ranging from 9.1 to 9.9, emphasizing the urgency of patching. Successful exploitation of these flaws could allow threat actors to execute arbitrary code or write arbitrary files.

The critical flaws are as follows:

- CVE-2024-38657 - An attacker with admin access can write arbitrary files in ICS with a CVSS score 9.1.
- CVE-2025-22467 - A buffer overflow in ICS allows for remote code execution with a CVSS score 9.9.
- CVE-2024-10644 - Code injection in ICS and IPS permits a remote attacker with admin privileges to execute code with a CVSS score 9.1.
- CVE-2024-47908 - Command injection in the CSA admin console with a CVSS score 9.1.

Health-ISAC strongly advises its members to prioritize patching vulnerabilities in Ivanti devices, as threat actors frequently target these systems for various motivations.

Recommendation:

- Apply available patches for vulnerable Ivanti devices.
- Ensure all of the devices are patched in a timely manner.
- Enforce network segmentation and strict network access control policies.
- Continuously monitor suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	HHS, The Hacker News, ivanti, ivanti, ivanti

Sources
https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html
https://www.ivanti.com/blog/february-security-update

Release Date
Feb 12, 2025 (UTC)

Alert ID 1cb78656

View Alert

Share Feedback
was this helpful? |

Tags CVE-2024-47908, CVE-2024-10644, CVE-2025-22467, CVE-2024-38657, Ivanti

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/**