THREAT BULLETINS

Critical Flaw in Ivanti's Cloud Services Appliance (CSA) is Being Exploited

TLP:WHITE

Sep 20, 2024

On September 19, 2024, Ivanti disclosed a critical vulnerability, CVE-2024-8963, in its Cloud Services Appliance (CSA), which is being exploited in targeted attacks.

The flaw is a patch traversal vulnerability affecting Ivanti's Cloud Services Appliance (CSA) 4.6 devices. In the event of a successful attack, adversaries can bypass administrative control and gain access to sensitive data. The flaw's CVSS score is 9.4, highlighting the urgency of patching. The patches were rolled out as part of September CSA 4.6 Patch 519 updates.

The attackers can chain CVE-2024-8963 with CVE-2024-8190, another high-severity CSA command injection bug, to bypass admin authentication and execute arbitrary commands on vulnerable devices. CVE-2024-8190 was originally reported on September 10, with the first exploitation attempts reported just a few days after the disclosure. CVE-2024-8963 was found after a more thorough investigation of the exploited CVE-2024-8190.

Reference(s)	ivanti, ivanti, socradar, socradar, Security Week

Recommendations

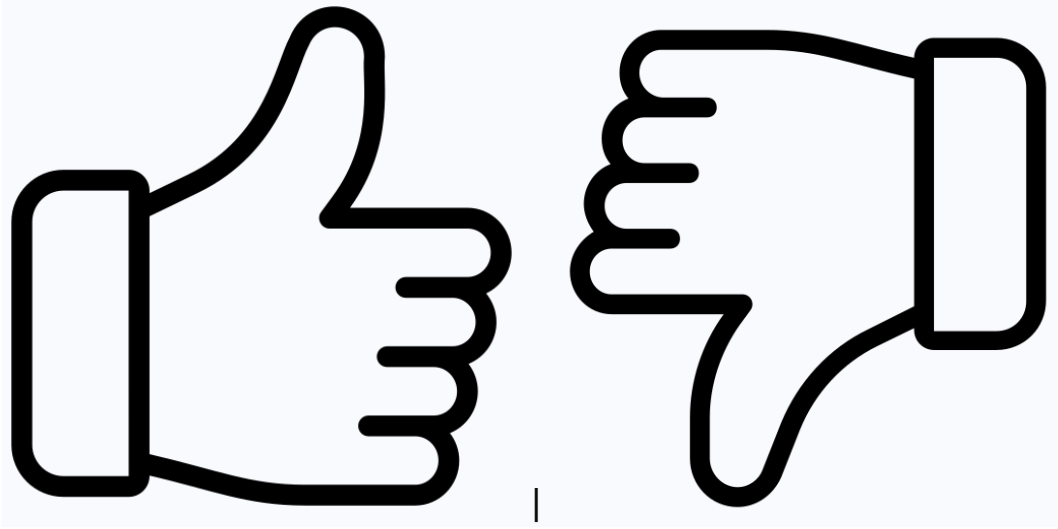
- Immediately upgrade to Ivanti CSA 5.0.
- Replace end-of-life devices with supported alternatives.
- Continuously monitor systems and logs for any sign of suspicious activity.
- Segment your network and limit network access to prevent lateral movement in case of a compromise.
- Develop an incident response plan to ensure business continuity in case of a successful cyberattack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Incident Date
Sep 19, 2024 (UTC)

Alert ID 5ec359f0

View Alert

Share Feedback
was this helpful?



Tags CVE-2024-8190, CVE-2024-8963, Ivanti CSA Flaw

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

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

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/**