TLP:CLEAR

U.S. COAST GUARD

MARITIME CYBER BULLETIN

31 January 2024

MCB 01-24: Critical Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities Identified

THREAT SUMMARY

Users of Ivanti Connect Secure and Ivanti Policy Secure solutions are vulnerable to known exploitations (CVE-2023-46805 and CVE-2024-21887) found in the web component of these solutions. These vulnerabilities allow an attacker to bypass control checks and authenticate as an administrator over the internet to move laterally, perform data exfiltration, establish persistent system access, and remotely gain control of the affected system. CISA rates this vulnerability as CRITICAL.

Recommendations

Ivanti mitigation steps require all agencies running Ivanti Connect Secure or Ivanti Policy Secure solutions to download and import "mitigation.release.20240107.1.xml", via Ivanti's download portal, into the affected product. Immediately after importing the XML file, agencies must download and run Ivanti's External Integrity Checker Tool.

For those using the affected products, please refer to the following references for further guidance:

- Recovery Steps Related to CVE-2023-46805 and CVE-2024-21887
- ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

Sources

"ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities." January 19, 2024. https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities.

Resources

Facilities that observe any unusual activity or interruptions to their network should report those activities per CG-5P Policy Letter 08-16 – Reporting Suspicious Activity and Breaches of Security to:

- Coast Guard's National Response Center
  1-800-424-8802

OR

Cybersecurity and Infrastructure Security Agency (CISA) Central
1-888-282-0870

If you have any questions, please visit our website at: https://www.uscg.mil/MaritimeCyber or reach out to MCRB at: maritimecyber@uscg.mil

The information contained in this bulletin is provided for **informational purposes only**. This information is based on common standards and best practices, the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information. Information Sharing Protocol: (https://www.us-cert.gov/tlp)