*CYBER ADVISORY*

TLP:CLEAR

04 April 2024

# Progress Flowmon Vulnerability

CVE-2024-2389 | RCE | DoS | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a severe critical vulnerability known as CVE-2024-2389.[1] The vulnerability affects Progress Flowmon versions 11.x and 12.x.[2] Exploitation of the vulnerability may allow an unauthenticated remote attacker to execute arbitrary code, read potentially sensitive memory, or create a denial-of-service (DoS) condition on affected devices.[3]

The Cal-CSIC recommends immediately upgrading to the appropriate patched version of Progress Flowmon.

For further information applying Progress Flowmon patches, please refer to Progress Kemp Technologies.

## 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. |

| | |
|---|---|
| **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] Security Week; "Critical Vulnerability in Progress Flowmon Allows Remote Access to Systems;" https://www.securityweek.com/critical-vulnerability-in-progress-flowmon-allows-remote-access-to-systems/; accessed 04 April 2024
[2] Run Zero; "How to find Progress Software Flowmon Packet Investigator with runZero;" https://www.runzero.com/blog/progress-software-flowmon/; accessed 04 April 2024
[3] Soc Radar; "Critical OS Command Injection Flaw in Progress Flowmon: CVE-2024-2389;" https://socradar.io/command-injection-flaw-progress-flowmon-cve-2024-2389/; accessed 04 April 2024