CYBER ADVISORY

TLP:CLEAR

08 August 2024

Progress WhatsUp Vulnerability

CVE-2024-4885 | Progress | Critical Vulnerability | Active Exploitation

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability that is under active exploitation known as CVE-2024-4885.[1] The vulnerability affects Progress WhatsUp Gold versions prior to 2023.1.3.[2] Exploitation of remote code execution (RCE) vulnerability in the 'WhatsUp.ExportUtilities.Export. GetFileWithoutZip' function, may allow an unauthenticated attacker to execute commands with the privileges of the 'iisapppool\\nmconsole' user.[3]

The Cal-CSIC recommends immediately upgrading to Progress WhatsUp Gold version 23.1.3.

For further information on applying upgrades please refer to Progress Community.

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] The Hacker News; "Critical Security Flaw in WhatsUp Gold Under Active Attack - Patch Now;" https://thehackernews.com/2024/08/critical-security-flaw-in-whatsup-gold.html; accessed 08 August 2024

[2] Bleeping Computer; "Critical Progress WhatsUp RCE flaw now under active exploitation" https://www.bleepingcomputer.com/news/security/critical-progress-whatsup-rce-flaw-now-under-active-exploitation/; accessed 08 August 2024

[3] Mitre; "CVE-2024-4885" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4885; accessed 08 August 2024