CYBER ADVISORY

TLP:CLEAR

3 January 2025

Progress WhatsUp Gold Three Critical Vulnerabilities Disclosed

Public API | LDAP | Progress | WhatsUp Gold

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two critical rated vulnerabilities and one medium rated vulnerability affecting WhatsUp Gold versions prior to 24.0.2. Exploitation of these vulnerabilities could lead to severe security risks including system takeover, unauthorized access to sensitive information, and data manipulation.[1]

The first, CVE-2024-12108 (CVSS 3.1 score of 9.6) is an authentication bypass vulnerability that can allow an attacker to gain access to the WhatsUp Gold server via the public API.[2] The second, CVE-2024-12106 (CVSS 3.1 score of 9.4) is a missing authentication for critical function vulnerability that allows an unauthenticated attacker to configure the Lightweight Directory Access Protocol (LDAP) settings.[3] The third, CVE-2024-12105 (CVSS 3.1 score: 6.5) is an improper limitation of a pathname to a restricted directory vulnerability that can allow an authenticated user to use a specially crafted HTTP request that can lead to information disclosure.[4]

The Cal-CSIC recommends immediately updating to the latest WhatsUp Gold version.

For more information on applying the security updates please refer to the Progress Community Advisory.

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 here.
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] Cybersecurity News; "CVE-2024-12108 (CVSS 9.6) and Beyond: Progress Issues Critical Patch for WhatsUp Gold Network Monitoring Software"; https://securityonline.info/cve-2024-12108-whatsup-gold-network-monitoring-software/; accessed 3 January 2025
[2] National Vulnerability Database; "CVE-2024-12108 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-12108; accessed 3 January 2025
[3] National Vulnerability Database; "CVE-2024-12106 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-12106; accessed 3 January 2025
[4] National Vulnerability Database; "CVE-2024-12105 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2024-12105; accessed 3 January 2025