Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2024-4885: Active Exploitation of Critical WhatsUp Gold RCE Flaw

Date of Publication	Admiralty Code	TA Number
August 8, 2024	A1	TA2024302

Summary

First Seen: April 24, 2024
Affected Product: Progress WhatsUp Gold
Impact: Multiple critical security flaws in Progress Software's WhatsUp Gold, particularly CVE-2024-4885, are being actively exploited. This flaw, present in versions before 23.1.3, allows unauthenticated remote code execution due to inadequate input validation in the GetFileWithoutZip function. A proof-of-concept exploit is publicly available, and Progress Software has released fixes, users are strongly urged to update to the latest version and restrict access to vulnerable endpoints.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4885	Progress WhatsUp Gold Remote Code Execution Vulnerability	Progress WhatsUp Gold	✗	✗	✓
CVE-2024-4884	Progress WhatsUp Gold Remote Code Execution Vulnerability	Progress WhatsUp Gold	✗	✗	✓
CVE-2024-4883	Progress WhatsUp Gold Remote Code Execution Vulnerability	Progress WhatsUp Gold	✗	✗	✓
CVE-2024-5008	Progress WhatsUp Gold Unrestricted Fie Upload Vulnerability	Progress WhatsUp Gold	✗	✗	✓
CVE-2024-5009	Progress WhatsUp Gold Improper Access Control Vulnerability	Progress WhatsUp Gold	✗	✗	✓

Vulnerability Details

#1

Multiple critical security flaws have been identified in Progress Software's WhatsUp Gold, with CVE-2024-4885 being actively exploited. This vulnerability, which has a CVSS score of 9.8, allows attackers to execute arbitrary code on affected systems without authentication. The flaw is found in versions released before 23.1.3 and originates from a weakness in the GetFileWithoutZip function, where inadequate input validation permits attackers to bypass security measures and upload malicious files to the server.

#2

The exploitation process involves crafting a specific request that manipulates the GetFileWithoutZip function, enabling the upload and execution of a malicious payload. Once uploaded, this payload can be triggered to execute arbitrary commands on the server, potentially giving the attacker control over the system. This control can lead to severe consequences, including unauthorized access, data theft, and the deployment of additional malware.

#3

This vulnerability is already being actively exploited in the wild, with reports from the Shadowserver Foundation indicating that attacks began on August 1, 2024. Alongside CVE-2024-4885, other vulnerabilities, such as CVE-2024-4883 and CVE-2024-5009, also have publicly available proof-of-concept (PoC) exploits.

#4

Progress Software has released fixes, urging users to update to version 23.1.3, which addresses CVE-2024-4885 along with two other critical vulnerabilities (CVE-2024-4883 and CVE-2024-4884) and two high-severity vulnerabilities (CVE-2024-5008 and CVE-2024-5009), all capable of remote code execution and privilege escalation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4885	WhatsUp Gold versions released before 2023.1.3	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*:*	CWE-22
CVE-2024-4884	WhatsUp Gold versions released before 2023.1.3	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*:*	CWE-94 CWE-77 CWE-78
CVE-2024-4883	WhatsUp Gold versions released before 2023.1.3	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*:*	CWE-94 CWE-77 CWE-78
CVE-2024-5008	WhatsUp Gold versions released before 2023.1.3	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*:*	CWE-434
CVE-2024-5009	WhatsUp Gold versions released before 2023.1.3	cpe:2.3:a:progress:whatsup_gold:2023.1.0:*:*:*:*:*:*:*	CWE-269

Recommendations

Update Software Immediately: Upgrade to WhatsUp Gold version 23.1.3 or later. This version addresses CVE-2024-4885, as well as other critical vulnerabilities, all of which pose significant security risks.

Restrict Access: Limit access to WhatsUp Gold instances to only trusted IP addresses and enforce strict authentication measures.

Monitor Network Traffic: Implement robust monitoring of network traffic for suspicious activity, especially targeting the /NmAPI/RecurringReport endpoint. Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to alert on and block unusual or unauthorized attempts to exploit this endpoint.

Segregate Networks: Network segmentation can help isolate vulnerable systems and prevent lateral movement if an attacker gains access. This practice is essential for maintaining the integrity of critical systems and data.

Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and mitigate potential security risks promptly.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0006 Credential Access	TA0004 Privilege Escalation
TA0007 Discovery	TA0005 Defense Evasion	TA0001 Initial Access	T1608 Stage Capabilities
T1068 Exploitation for Privilege Escalation	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1210 Exploitation of Remote Services
T1203 Exploitation for Client Execution	T1202 Indirect Command Execution	T1608.002 Upload Tool	

Patch Details

Upgrade WhatsUp Gold version to 23.1.3 or later.

Links:
https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024

References

https://summoning.team/blog/progress-whatsup-gold-rce-cve-2024-4885/

https://github.com/sinsinology/CVE-2024-4885

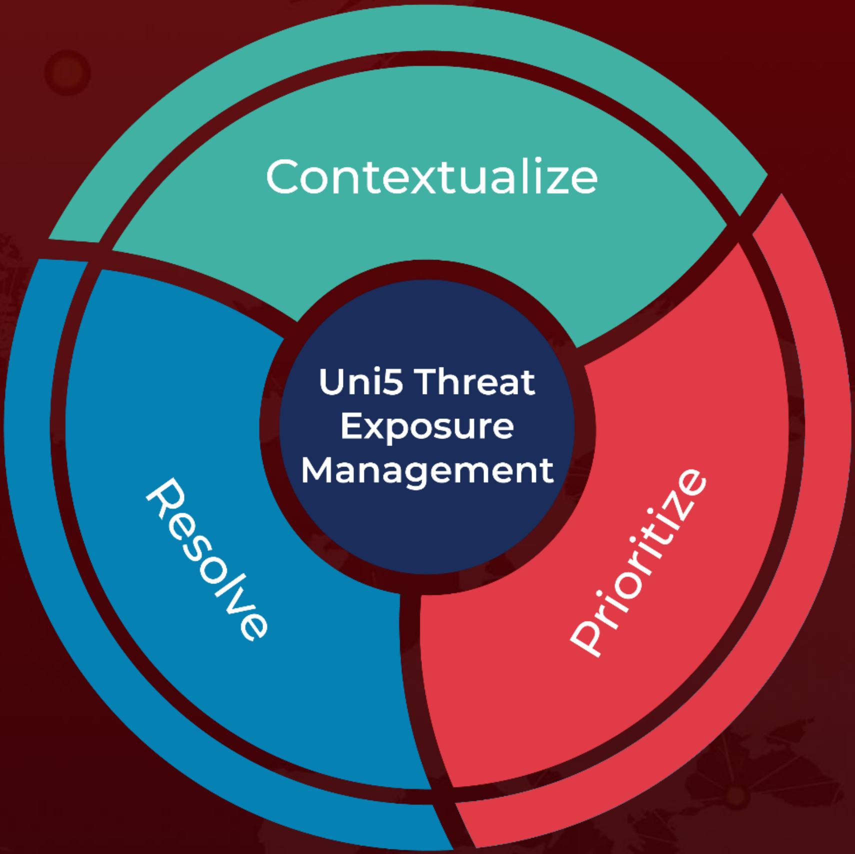
https://github.com/sinsinology/CVE-2024-4883

https://github.com/sinsinology/CVE-2024-5009

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 8, 2024 • 5:30 AM

More at www.hivepro.com